UNIVERSIDAD DE PANAMÁ

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

LA RESPONSABILIDAD CIVIL DE LOS BANCOS EN RAZÓN DEL HECHO INFORMATICO

CARLOS L. QUINTERO S.

TESIS PRESENTADA COMO UNO DE LOS REQUISITOS PARA OPTAR A LA MAESTRÍA EN DERECHO CON ESPECIALIZACIÓN EN DERECHO PRIVADO

PANAMÁ, REPÚBLICA DE PANAMÁ

1997

DEDICATORIA

A DIOS

A MI MADRE, CRISTINA Y A MI PADRE CARLOS

CONTENIDO

RESUMEN 1

INTRODUCCIÓN 2

REVISIÓN DE LITERATURA O FUNDAMENTACIÓN TEÓRICA 11

ASPECTOS METODOLÓGICOS 14

RESULTADOS Y DISCUSIÓN 16

CAPÍTULO PRIMERO: CONSIDERACIONES GENERALES SOBRE LA RESPONSABILIDAD CIVIL Y DE LA ACTIVIDAD BANCARIA

I. CONSIDERACIONES GENERALES SOBRE LA RESPONSABILIDAD CIVIL 17

A. CONCEPTO DE RESPONSABILIDAD CIVIL 17
B. RESPONSABILIDAD CONTRACTUAL Y EXTRACONTRACTUAL 18
C. DIFERENCIAS ESPECÍFICAS ENTRE LA RESPONSABILIDAD CONTRACTUAL Y LA EXTRACONTRACTUAL 19
1. En cuanto a su origen 19
2. En cuanto a la gradación de la culpa 20
3. En cuanto a la solidaridad 21
4. En materia de carga de la prueba 21
5. En razón de la extensión del resarcimiento 22
6. En materia de mora 22
7. En cuanto a la atenuación de la responsabilidad 23
8. En cuanto a la prescripción 24
D. SUB-DIVISIONES EN LA RESPONSABILIDAD CIVIL CONTRACTUAL Y EN LA EXTRACONTRACTUAL 24
E. ELEMENTOS COMUNES 25
1. La antijuridicidad 25
2. El daño 25
3. La relación de causalidad 27
4. Factores de imputabilidad 28
(a) Factores subjetivos de imputabilidad 28
(b) Factores objetivos de imputabilidad 29
F. LA RESPONSABILIDAD PROFESIONAL 32

II. CONSIDERACIONES GENERALES SOBRE LA RESPONSABILIDAD CIVIL DE LOS BANCOS 35

A. NATURALEZA DE LA RESPONSABILIDAD 35
B. BIENES E INTERESES JURÍDICOS SUSCEPTIBLES DE DAÑO POR EL ACTUAR DEL BANCO 42

III. LA ACTIVIDAD BANCARIA COMO DETERMINANTE DE LA RESPONSABILIDAD CIVIL DE LOS BANCOS 43

A. EL CARÁCTER COMERCIAL O MERCANTIL 44
B. LA INTERMEDIACIÓN 45

C. LA MASIVIDAD 46
D. LA ADHESIVIDAD CONTRACTUAL 48
E. LA PROFESIONALIDAD 52
F. EL RIESGO 53
G. LA INTEGRACIÓN EN UN SISTEMA 54
H. EL SERVICIO PÚBLICO 54
I. EL SECRETO BANCARIO 56

CAPÍTULO SEGUNDO: ASPECTOS GENERALES DE LA RESPONSABILIDAD DEL BANCO FRENTE AL HECHO INFORMÁTICO

I. EL HECHO INFORMÁTICO BANCARIO 60
A. CONCEPTO 60
B. FINALIDAD DE LA INFORMÁTICA BANCARIA 63
C. LA TRANSFERENCIA ELECTRÓNICA DE FONDOS 69
D. OTRAS APLICACIONES DEL PROCESAMIENTO ELECTRÓNICO DE DATOS Y ALGUNOS DE SUS EFECTOS EN LA ACTIVIDAD BANCARIA 74
E. LA INFORMÁTICA BANCARIA EN PANAMÁ 78
II. NATURALEZA JURÍDICA DE LA RESPONSABILIDAD DE LOS BANCOS FRENTE AL HECHO INFORMÁTICO BANCARIO 81
A. RESPONSABILIDAD CONTRACTUAL 82
B. RESPONSABILIDAD EXTRACONTRACTUAL 88
C. NATURALEZA DE LA RESPONSABILIDAD TRATÁNDOSE DE LA GESTIÓN DE BANCOS DE DATOS 94
D. LIMITACIÓN O EXONERACIÓN DE LA RESPONSABILIDAD DEL BANCO EN FUNCIÓN DE SU NATURALEZA OBJETIVA O SUBJETIVA 98
III. ELEMENTOS DE LA RESPONSABILIDAD 101
A. LA ANTIJURIDICIDAD 101
B. EL DAÑO 102
C. NEXO DE CAUSALIDAD 104
D. FACTORES DE ATRIBUCIÓN 106
IV. OBLIGACIONES ESPECIALES DE LOS BANCOS FRENTE A SUS CLIENTES EN RAZÓN DEL HECHO INFORMÁTICO 106
A. OBLIGACIONES LEGALES 107
1.OBLIGACIÓN DE RENDIR CUENTAS 107
2. OBLIGACIONES DE RESERVA 110
B. OBLIGACIONES TÉCNICAS 113
V. LA INTERNACIONALIZACIÓN DEL HECHO INFORMÁTICO BANCARIO 125
A. CONSIDERACIONES GENERALES 125
B. TRANSFERENCIAS ELECTRÓNICAS DE FONDOS A NIVEL INTERNACIONAL 127
C. LEY APLICABLE 129

CAPÍTULO TERCERO: BIENES E INTERESES JURÍDICOS AFECTADOS Y SUPUESTOS DE RESPONSABILIDAD DEL BANCO

I. BIENES E INTERESES JURÍDICOS AFECTADOS 131
A. EL PATRIMONIO 131

1. La responsabilidad patrimonial por las transferencias electrónicas de fondos: la legislación de los Estados Unidos de América 132
2. La responsabilidad patrimonial en las nuevas tecnologías bancarias 145
B. LA INTIMIDAD 146
1. Concepto y alcance 146
2. Intimidad e informática bancaria 150
3. Regulación jurídica de la intimidad y la informática 155
(a) Evolución de la legislación 155
(b) Contenido de la legislación: la protección de la intimidad a través de la protección de los datos personales 162
(c) Tratamiento del tema por parte de los organismos internacionales 171
4. Limitaciones al derecho a la intimidad en la informática bancaria 173

C. EL SECRETO O RESERVA 182
D. EL HONOR 183
E. LA IDENTIDAD PERSONAL 185
II. SUPUESTOS DE RESPONSABILIDAD DEL BANCO 187
A. PÉRDIDA TOTAL O PARCIAL DE LA INFORMACIÓN 189
B. ALTERACIÓN DE LA INFORMACIÓN SOBRE LOS CLIENTES 190
C. EL ACCESO, LA SUSTRACCIÓN Y LA DIVULGACIÓN DE DICHA INFORMACIÓN POR TERCEROS NO AUTORIZADOS 199

CONCLUSIONES Y RECOMENDACIONES 201

I. CONCLUSIONES 201
II. RECOMENDACIONES 217

BIBLIOGRAFÍA 224

RESUMEN

Partiendo de un método deductivo y un enfoque descriptivo, hemos examinado los aspectos generales de la responsabilidad civil, encontrando diferencias esenciales entre la responsabilidad civil contractual y la extracontractual, así como la existencia de peculiaridades de la responsabilidad civil dentro del ámbito bancario. También se ha determinado que de alguna forma, los elementos de la actividad bancaria condicionan la responsabilidad civil de los bancos. La existencia de un hecho informático bancario que hace que los bancos deban asumir un tipo especial de responsabilidad para con sus clientes, también ha sido parte de nuestras conclusiones. Esta responsabilidad ha sido objeto de diferentes explicaciones y teorías por parte de quienes han estudiado esta situación. Igualmente hemos concluido que los bancos deben asumir obligaciones específicas tanto en el ámbito bancario como en el técnico, para no incurrir en la mencionada responsabilidad. Un hecho importante ha sido el determinar los efectos que la internacionalización del hecho informático bancario produce en las relaciones jurídicas de los estados, máxime cuando éstos mantienen diferencias en cuanto a la protección de los derechos de sus ciudadanos frente a los riesgos de la tecnología. Tal situación tiene especial importancia por cuanto que el hecho ilícito informático afecta distintos bienes e intereses jurídicos de las personas, tales como el patrimonio, la intimidad, el honor y la identidad personal, lo cual ha determinado que numerosos países protejan los derechos de sus ciudadanos especialmente en el ámbito civil, mientras que otros aun carecen de legislaciones en este sentido. Se tienen como los principales supuestos de responsabilidad de los bancos en esta materia, hechos tales como: la pérdida total o parcial de la información, la alteración de la información sobre los clientes y el acceso, la sustracción y la divulgación de dicha información por terceros no autorizados.

ABSTRACT

Using the deductive method and a descriptive approach to the subject, an examination was made of the general features of civil liability, arriving at the essential differences between civil liability which arises out of contracts and extracontractual civil liability, as well as the existence of features that are peculiar to civil liability within the realm of banking activities. It was also found that, to some extent, the components of banking activities condition the civil liability of banks. One of the most important conclusions of the research is that the existence itself of computerised banking data is responsible for the banks having to assume a special kind of liability with regard to their clients. Said liability has been the subject of different explanations and theories put forth by those who have studied the matter in detail. Likewise, we have concluded from our research that banks must assume specific obligations both within the field of banking and the field of technology, in order to avoid incurring said liability. An important feature has been the determination of the effects that the internationalization of computerized banking data has had on the juridical relations between states, especially in cases where differences exist in the way in which each state protects the rights of its citizens vis-à-vis the risks posed by technology. This situation is particularly relevant inasmuch as their personal estate, the right to privacy, banking secrecy, and their honor and personal identity, thereby leading numerous countries to offer protection to the rights of their citizens, especially within the realm of the civil law, while still other countries lack the laws that provide such protection. The principal causes of liability by banks regarding this matter are such acts as: the total or partial loss by the banks of banking data on their clients, the unlawful and intentional alteration of client data by the banks, and the unlawful access, removal and disclosure of said information by unauthorized third parties.

INTRODUCCIÓN

El tema de la responsabilidad civil de los bancos ha sido poco estudiado en nuestro medio, a pesar de que nuestro país se considera un centro bancario a nivel internacional, en el cual operan un número considerable de instituciones bancarias que desarrollan una pluralidad de operaciones de orden diverso.

Los bancos como empresas que incursionan en el ámbito de la economía de servicios son sujetos de actividades que los hacen asumir importantes obligaciones con sectores diversos de la población, ya sea a nivel individual o sectorial (la agricultura, la industria, el comercio, etc.). La masividad propia de la actividad bancaria determina que el nivel de riesgo, es decir la posibilidad de que sus clientes como contrapartes de esa actividad sufran daños de naturaleza diversa con el accionar del banco, resulte mucho mayor que aquél que puede advertirse en las actividades de otro tipo de empresas de servicio.

Ahora bien, la actividad bancaria, en virtud de la forma masiva que adopta y la necesidad de optimar sus servicios, requiere hacer uso de los mayores adelantos tecnológicos para el registro y desarrollo de sus operaciones, lo cual determina que la responsabilidad civil en que la misma incurra por los daños que ocasione a sus clientes o terceros, los cuales debe correlativamente reparar, sea ocasionada en muchos casos por el uso negligente o mal intencionado de tales instrumentos tecnológicos e inclusive, por no reunir dichos instrumentos, los requisitos indispensables para el cumplimiento de su finalidad. Y es que estos instrumentos determinan también la creación de nuevos y mayores riesgos en la producción de determinados daños, que los instrumentos convencionales de registro de información.

Ninguna entidad bancaria de nuestro tiempo puede prescindir en tal sentido de la informática, es decir del tratamiento electrónico de sus operaciones, si quiere competir con alguna posibilidad de éxito en el sistema bancario tanto a nivel nacional como internacional. De allí que la generalidad de las entidades bancarias procesen a través de sus propios centros de informática, miles o en algunos casos millones de operaciones diariamente, las cuales incluyen datos sobre el patrimonio o la identidad de sus clientes. Es así que estos hechos informáticos y principalmente la pérdida, alteración, acceso, sustracción o divulgación de la información electrónicamente tratada, produzca una lesión al patrimonio, la intimidad, el secreto, el honor o la identidad personal de sus clientes por acción directa del tratamiento que los mismos tengan por parte del banco, supondrán nuevos deberes para las entidades bancarias tendientes a evitar diversos supuestos de responsabilidad en que las mismas puedan incurrir.

Nuestra investigación ha tratado de analizar la responsabilidad de naturaleza civil que para las entidades bancarias supone el tratamiento electrónico de sus operaciones, o sea los denominados hechos informáticos en materia bancaria.

En nuestro estudio de la responsabilidad civil derivada de los hechos informáticos, hemos advertido que muchos teóricos y legislaciones extranjeras se han concentrado principalmente en lo que atañe al tratamiento electrónico de la llamada información nominativa. Es decir, aquella que trata los aspectos relativos a la identidad y condiciones particulares de las personas y cómo el uso inadecuado o abusivo de esta información lesiona los derechos de la personalidad.

Tanto la doctrina como la legislación de diversos países han incursionado en el análisis de este aspecto a través de las denominadas leyes de datos. La lesión del derecho a la intimidad por la divulgación no autorizada de información personal constituye un

problema cuyo análisis ha sido tratado en función del tratamiento automatizado de dicha información.

No obstante lo anterior, a través de nuestro estudio, hemos concluido que a través del uso de las herramientas tecnológicas que nos brinda la informática, no sólo se procesa información nominativa, sino también información de la más variada naturaleza, incluyendo aquella referente al patrimonio de las personas. Esto último ocurre principalmente con el manejo y registro electrónico de las operaciones bancarias tanto activas (préstamos, líneas de crédito, etc.) como pasivas (depósitos irregulares), de cuya corrección y seguridad dependerá en gran medida la posición financiera de los clientes de la entidad bancaria.

Sobre la responsabilidad civil que el banco debe asumir, en razón del posible daño que se ocasione al cliente como consecuencia del tratamiento electrónico de sus operaciones, poco se ha escrito en el ámbito latinoamericano. Consideramos pertinente resaltar los estudios elaborados a nivel de la Federación Latinoamericana de Bancos (FELABAN), los cuales entran a analizar diversos aspectos legales relacionados con la aplicación de la informática en la actividad bancaria. También son trascendentes los estudios elaborados por la Comisión de las Naciones Unidas para el derecho mercantil internacional (UNCITRAL). En lo que al aspecto legislativo se refiere, existen pocos ordenamientos jurídicos que en nuestra región, regulan la responsabilidad bancaria en lo relativo a lo que podríamos denominar la informática bancaria, en este sentido deben destacarse los ordenamientos constitucionales de Colombia, Chile y Brasil y los proyectos de ley de Chile y Argentina. En los otros países debe recurrirse, en todo caso, a disposiciones de carácter genérico para solucionar los problemas que se presentan.

En cuanto a la importancia del presente estudio, es preciso señalar que en Panamá como Centro Bancario Internacional, en el cual operan cerca de un centenar de

entidades bancarias que efectúan actividades tanto a nivel local como internacional, se recurre a la informática o sea el tratamiento electrónico de las operaciones bancarias, que en un día pueden sumarse por miles. La pérdida, alteración o fuga de la información financiera y aún de naturaleza personal de los clientes que es electrónicamente procesada y registrada, puede afectar a éstos de forma sensible en aspectos tales como el nivel de solvencia económica, su capacidad como sujetos de crédito y su imagen personal en la comunidad. Así la determinación de los elementos esenciales de la responsabilidad civil de los bancos, sus principales deberes, los bienes e intereses jurídicos afectados y aquellas situaciones en las que puede surgir una responsabilidad civil para éstos en razón de hechos informáticos, resulta de relevante importancia.

En adición a lo anterior, la falta de una adecuación de la legislación penal y la inexistencia de una legislación administrativa que tutele ya sea los derechos del Estado, la sociedad o los particulares en esta materia, dan por resultado que sea la legislación civil, el único amparo de quien busca una reparación por el daño infringido a sus derechos.

En cuanto a las hipótesis que nos puede presentar el problema planteado serían esencialmente dos, a saber: que existe una responsabilidad civil de los bancos para con sus clientes, en razón del hecho informático o que no existe tal responsabilidad. Nuestra intensión en el presente estudio ha sido demostrar que si existe tal responsabilidad y pretendemos explicar en qué consiste la misma. En tal sentido, hemos comprobado a nivel de la doctrina y de la legislación interna y extranjera, que en razón del tratamiento electrónico de sus operaciones, los bancos deben asumir ciertos deberes para con sus clientes, deberes estos que de no ser observados provocarán situaciones en las cuales

dichas entidades se verán obligadas a reparar los daños tanto morales como patrimoniales que ocasionen a sus clientes.

Los objetivos alcanzados con nuestro estudio han sido entre otros:

1. Describir en forma breve la responsabilidad civil que surge para los bancos en razón de la actividad bancaria que realizan, tanto en su forma contractual como extracontractual.

2. Sustentar y analizar la existencia de una responsabilidad civil que surge para los bancos en razón del procesamiento electrónico de la información que reciben sobre sus clientes, a propósito de las operaciones y los contratos bancarios de los cuales éstos forman parte y cómo la existencia de tal responsabilidad repercute en la creación o aplicación del derecho.

3. Establecer y examinar la naturaleza y los elementos principales de la responsabilidad civil de los bancos, en razón del procesamiento electrónico de la información que recibe sobre sus clientes, a la luz de la doctrina y la ley.

4. Establecer y examinar los principales deberes que deben asumir los bancos en virtud del procesamiento electrónico de la información que reciben sobre sus clientes, conforme a las principales fuentes del derecho.

5. Establecer y examinar los bienes e intereses jurídicos que resultan afectados con los hechos ilícitos informáticos.

6. Establecer y examinar aquellas situaciones específicas que catalogamos como supuestos fácticos de la responsabilidad civil de los bancos, en razón del procesamiento electrónico de la información que reciben sobre sus clientes, tal y como lo plasman los usos, los contratos, las reglamentaciones bancarias, la legislación nacional y comparada y la jurisprudencia.

Aunque consideramos que ello se infiere de los mencionados objetivos, queremos reafirmar que se analiza la responsabilidad de los bancos exclusivamente en lo que atañe a sus clientes, precisión que se hace necesaria a fin de que se tome en cuenta que la responsabilidad que pudiese dimanar como consecuencia de la afectación de bienes o intereses jurídicos protegidos de otros posibles afectados con la actividad informática bancaria, tal y como lo podrían ser los accionistas del banco, el Estado u otras personas distintas de los clientes, no es objeto del presente estudio.

En lo que respecta al contenido de cada uno de los capítulos que sustentan la hipótesis planteada en el presente estudio tenemos que:

En el primer capítulo hacemos ciertas consideraciones generales cobre la responsabilidad civil general y de la actividad bancaria. Partimos por analizar las características de la responsabilidad civil de forma comparativa y en función de la existencia de una responsabilidad civil contractual y una responsabilidad civil extracontractual. En este sentido, comentamos lo relacionado con el origen de las responsabilidades, la gradación de la culpa, la solidaridad de los obligados, las diferencias existentes en materia de carga de la prueba, la extensión del resarcimiento que surge como resultado del daño causado, las diferencias existentes en materia de la mora en el cumplimiento de las obligaciones, las posibilidades de atenuación de la responsabilidad por vía contractual o en el ámbito extracontractual y el reconocimiento legislativo a tales fórmulas, además de lo relacionado con la prescripción de las acciones.

Comentamos igualmente lo relacionado con la responsabilidad civil de los bancos en particular, definiendo la naturaleza de la misma y los bienes e intereses jurídicos que resultan susceptibles de daño por el actuar del banco, así también enumeramos una serie de situaciones en las cuales la jurisprudencia internacional ha

reconocido la existencia de una responsabilidad civil de los bancos para con sus clientes.

Examinamos como los diferentes elementos de la actividad bancaria determinan la existencia de la responsabilidad civil de los bancos, incluyendo su carácter comercial, su función intermediadora, su masividad, la adhesividad como característica de sus contratos, la profesionalidad de la actividad, el factor riesgo, la integración de los bancos dentro de un sistema, su carácter de servicio público y el secreto bancario.

En el capítulo segundo nos referimos a los aspectos generales de la responsabilidad del banco frente al hecho informático. En un inicio definimos el concepto de hecho informático bancario y seguimos con la determinación de la finalidad de la informática bancaria, ponemos especial énfasis en las operaciones de transferencias electrónicas de fondos y otras aplicaciones del procesamiento electrónico de datos y sus efectos en la actividad bancaria. En forma sintética efectuamos una breve reseña sobre la evolución de la informática bancaria en Panamá.

En otra sección examinamos lo relativo a la naturaleza jurídica de la responsabilidad de los bancos frente al hecho informático bancario, incluyendo el ámbito de la responsabilidad contractual y extracontractual, así como la trascendencia de la responsabilidad dimanante de la gestión de los bancos de datos y las posibilidades de limitar o exonerar la responsabilidad del banco en función de su naturaleza objetiva o subjetiva.

Se describe la forma en la que la informática influye en los distintos elementos de la responsabilidad civil de los bancos, es decir: la antijuridicidad, el daño, el nexo de causalidad y los factores de atribución.

También resultan objeto de nuestro estudio, los deberes especiales de los bancos frente a sus clientes en razón del hecho informático, tanto en el aspecto legal, en el cual

incluimos la obligación de rendir cuentas y la obligación de reserva, así como en el aspecto técnico, las cuales resultan numerosas en virtud de lo sofisticado de la nueva tecnología.

Concluimos este capítulo con una alusión al problema de la internacionalización del hecho informático bancario.

En el capitulo tercero tratamos de establecer los bienes e intereses jurídicos afectados con los hechos ilícitos informáticos y la forma en la que los mismos pueden ser afectados.

En razón de lo anterior, examinamos como resulta afectado el patrimonio, en especial por las transferencias electrónicas de fondos, materia ampliamente regulada en la legislación de los Estados Unidos de América, a la cual nos referimos en detalle. Igualmente nos referimos brevemente, a la forma en que este bien puede ser afectado por las nuevas tecnologías bancarias.

Una gran parte del capítulo, lo dedicamos a analizar la forma en que resulta afectado el bien jurídico intimidad. Para tales efectos conceptualizamos dicho bien y definimos su alcance, planteamos la relación existente entre el bien jurídico intimidad y la informática bancaria, igualmente detallamos ampliamente la regulación que la intimidad tiene en los derechos positivos extranjeros y a nivel de la legislación internacional, incluyendo la evolución de tal regulación, el contenido de la misma en función de la protección de los datos personales electrónicamente tratados y finalmente nos referimos a las limitaciones de la intimidad en la informática bancaria, incluyendo reseñas jurisprudenciales que en la práctica han planteado una solución a este problema.

Otros bienes jurídicos susceptibles de afectación que son tratados en este estudio resultan ser el secreto bancario, honor y la identidad personal.

En una última sección se tratan los supuestos de responsabilidad de los bancos, es decir: la pérdida total o parcial de la información de los clientes, la alteración de la misma, así como el acceso, la sustracción y la divulgación de dicha información a terceros no autorizados.

REVISIÓN DE LITERATURA O FUNDAMENTARON TEÓRICA.

Durante la elaboración de la presente tesis, hemos encontrado que existe un incipiente interés, sobre todo a nivel de América Latina, en el estudio de la responsabilidad civil y también penal de la actividad informática en general. No obstante, en muchos casos, las producciones jurídicas que encontramos, hacen énfasis en los aspectos filosóficos del problema que plantea el desarrollo de las nuevas tecnologías a las ciencias jurídicas. Así sucede por ejemplo con las obras del Doctor Vitorio Frosini y Messina de Estrella Gutiérrez, las cuales analizan la forma en la que el mencionado desarrollo influye tanto en la sociedad como en el ámbito particular del derecho.

Otras obras tienden a resaltar más que nada, lo que atañe a los denominados contratos informáticos, lo cual incluye su contenido, sus peculiaridades y las dificultades que en los mismos encuentran los consumidores de servicios informáticos, por su ignorancia en los intrincados aspectos técnicos de la informática. En tal sentido mencionamos las obras de Correa y Giannantonio.

En adición a lo anterior, ha surgido en forma reciente, una corriente literaria que pugna por resaltar la importancia del problema que plantea la informática en el aspecto probatorio, es decir en el ámbito del derecho procesal.

Lo relacionado con la responsabilidad civil derivada de la actividad informática o hechos informáticos, como nosotros hemos preferido denominarlos, no ha despertado aun el suficiente interés de los juristas de nuestro subcontinente latinoamericano, tal vez, por la poca importancia que hasta ahora se ha venido dando en nuestros países al asunto de la protección de los consumidores, incluyendo lo que podríamos denominar consumidores de servicios informáticos o de servicios realizados por medios

AGRADECIMIENTO

AL PROFESOR OCTAVIO DEL MORAL

informáticos, como es el caso de los consumidores de servicios financieros, incluyendo los bancarios.

Algunos se han preocupado más que nada, por tratar de solucionar el problema de estos consumidores, dándole un enfoque penal al problema. De estar forma se han escrito obras que promueven la adaptación de la legislación penal o la promulgación de normas que establezcan nuevos tipos penales que describan las actividades que se han dado en llamar delitos informáticos. Son de resaltar las obras de Guerrero Mateus y Santos Mora y la de chileno Jijena Leiva.

También tenemos a los que consideran que el problema debe ser analizado desde el punto de vista de los derechos humanos o del derecho constitucional de cada país, pues la denominada autodeterminación informática según ellos, es un derecho fundamental de los individuos, pues el mismo se deriva del derecho a la intimidad. Esto se advierte particularmente en la obra del mexicano Meján.

Pero en lo que a la responsabilidad civil respecta, tratándose de los hechos informáticos, consideramos que la misma no ha sido estudiada lo suficiente. Es un hecho que la inmensa mayoría de los autores coinciden en aceptarla aunque de diferentes formas. Algunos, como en el caso de Bustamante Alsina, reduciéndola a una responsabilidad subjetiva que tiene por objeto la protección de los llamados datos nominativos, o sea aquellos que guardan relación con la identidad personal. Otros dándole un enfoque objetivo fundado en la teoría del riesgo, como en el caso de las obras de Parellada, Delpiazzo, Borda, Bergel y los escritos de la Dra. Glen de Tobón.

Finalmente, hay quienes propugnan por efectuar un análisis de derecho comparado, con el fin de que buscar la armonización de los derechos nacionales de los distintos países a fin de encontrar una uniformidad, sin que falten los que propongan la celebración de tratados internacionales sobre la materia. Véase en este sentido los

trabajos elaborados a nivel de la Federación Latinoamericana de Bancos (FELABAN) y de la Comisión de las Naciones Unidas para el derecho mercantil internacional (UNCITRAL).

ASPECTOS METODOLOGICOS

Con el propósito de alcanzar los objetivos de nuestro trabajo, hemos recurrido al método deductivo, es decir hemos partido del establecimiento y análisis de los aspectos generales del problema planteado, para concluir con los aspectos particulares del mismo. Ello se refleja claramente en el orden y distribución de los capítulos de la presente tesis, la cual parte de los aspectos generales de la responsabilidad civil y luego profundiza en los aspectos particulares de la responsabilidad civil de los bancos derivada de los hechos ilícitos informáticos.

En cuanto al método de enfoque, recurrimos principalmente al método descriptivo. Para ello nos abocamos a examinar la principales características del problema escogido, su definición y la formulación de la hipótesis correspondientes, los supuestos fácticos del problema, así también hemos señalado las fuentes en que nos hemos basado para sustentar dicha hipótesis y hemos incluido la temática necesaria para describir todos los aspectos del problema planteado.

No obstante lo anterior, en algunos aspectos del tema objeto de nuestro estudio, tales como la evolución de la informática en el campo bancario a nivel mundial y nacional, hemos hecho uso del método histórico, ya que lo importante era establecer el impacto que en las operaciones bancarias, a tenido el desarrollo de la tecnología informática y como ello se refleja en el plano jurídico. También hemos empleado el método histórico, con la finalidad de explicar con mayor claridad la evolución legislativa en cuanto a la protección del bien jurídico intimidad, a través de la protección de la información electrónicamente tratada.

En lo que atañe a las diferencias existentes entre los dos grandes ámbitos de la responsabilidad civil, o sea el contractual y el extracontractual, así como aquellas que surgen de la clasificación en responsabilidad objetiva o subjetiva, principalmente en lo corresponde a su aplicación a la responsabilidad de los bancos derivada de un hecho ilícito informático, hemos recurrido a un método de enfoque de carácter comparativo.

RESULTADOS Y DISCUSIÓN

CAPÍTULO PRIMERO: CONSIDERACIONES GENERALES SOBRE LA RESPONSABILIDAD CIVIL Y DE LA ACTIVIDAD BANCARIA

I. Consideraciones Generales sobre la Responsabilidad Civil.

A. Concepto de Responsabilidad Civil.

La responsabilidad civil en términos generales implica en todo caso un deber de responder por parte de quien a causado un daño a favor de aquel a quien se le ha causado dicho daño. Debe entenderse que el daño implica "el menoscabo que, a consecuencia de un acaecimiento o evento determinado, sufre una persona, ya en sus bienes vitales naturales, ya en su propiedad, ya en su patrimonio" (Zannoni, 1993:1). Sin embargo, no siempre la sola causación del daño resulta suficiente para hacer surgir la responsabilidad del causante del mismo. Esto es así, porque para que el actuar o no actuar lesivo produzca un daño que haga surgir una responsabilidad civil, se requiere que dicha conducta sea contraria a la ley, es decir, que sea ilícita. Esta ilicitud debe manifestarse como un actuar contrario al ordenamiento jurídico, es decir que al momento de definir la ilicitud de la conducta no se puede atender a una norma o conjunto aislado de normas sino que se tiene que tomar en cuenta el cuerpo jurídico en su conjunto porque las disposiciones legales integran un sistema que debe ser analizado integralmente y no solo en función de una de las partes o elementos que lo componen. Y es que el sistema jurídico así como contempla las normas aplicables, también contempla las excepciones a las conductas genéricas previstas en las mismas. Entre estas últimas tenemos al estado de necesidad, la legítima defensa, la fuerza mayor y el caso fortuito.

Ahora bien, el actuar dañoso o lesivo tiene el efecto previsto por la ley bajo la forma de una sanción o de una indemnización. En el primer caso, para los efectos de retrotraer las cosas o el patrimonio a la forma original que tenían antes de ocasionada la responsabilidad civil, en contraposición de la represiva propia de la responsabilidad penal) y en el segundo, para los efectos de pagar una suma de dinero equivalente al daño sufrido.

En síntesis, podríamos decir que la responsabilidad civil es aquella que surge como resultado de una conducta positiva o negativa que ocasiona un daño y que contraviene el ordenamiento jurídico ocasionando que el autor de tal conducta deba cumplir una sanción o indemnizar al ofendido, en ambos casos según las previsiones legales aplicables.

B. Responsabilidad Contractual y Extracontractual.

La responsabilidad civil como otros conceptos complejos del derecho, presenta divisiones fundamentadas en elementos distintivos que permiten clasificarla. Así la responsabilidad civil se clasifica en responsabilidad contractual y responsabilidad extracontractual.

La responsabilidad civil contractual implica la necesaria existencia de un vínculo jurídico preexistente entre el autor del hecho dañoso y la víctima del mismo, vínculo este del cual surgen una o varias obligaciones para una o ambas partes y las cuales a la postre resultan siendo objeto de incumplimiento, lo que provoca un daño que siendo ilícito debe ser reparado.

Por su parte la responsabilidad civil extracontractual implica, en sentido contrario, la inexistencia de vínculo contractual entre el autor del daño ilícito y la víctima del mismo.

Es por ello que tratándose de la responsabilidad contractual se hace referencia a una obligación preexistente que resulta incumplida y en lo referente a la responsabilidad extracontractual estamos en presencia de una obligación que surge en el mismo momento en que se produce el daño, es decir de una obligación que no existía antes del ilícito, de una obligación nueva.

Nuestro Código Civil diferencia entre la responsabilidad contractual y la extracontractual. Es así que la responsabilidad contractual es regulada en el título primero del libro cuarto del Código Civil, específicamente entre los artículos 986 a 993, mientras que la responsabilidad civil extracontractual es prevista en el capítulo segundo del título decimosexto del libro cuarto, artículos 1644 a 1652 del Código.

C. Diferencias específicas entre la Responsabilidad Contractual y la Extracontractual.

En lo específico, la responsabilidad civil contractual y extracontractual presentan diferencias claras en aspectos diversos tales como:

1. En cuanto a su origen.

Como ya advertimos la responsabilidad contractual requiere de un vínculo jurídico preexistente entre dos o más personas que resultan obligadas a la realización de

una prestación, obligación esta que al ser incumplida da lugar al surgimiento de dicha responsabilidad. Por su parte la responsabilidad civil extracontractual surge de una hecho ilícito que da lugar al surgimiento de una obligación nueva y posterior a dicho hecho, la obligación de responder por el daño causado.

2. En cuanto a la gradación de la culpa.

En materia contractual, se hace referencia a diversos grados de culpa. Así el artículo 34 c del Código Civil hace alusión a tres, a saber:

Culpa grave, negligencia grave o culpa lata, la cual consiste en no manejar los negocios ajenos con aquel cuidado que aun las personas negligentes o de poca prudencia suelen emplear en sus negocios propios. Esta culpa es equivalente al dolo en materia civil.

Culpa leve, descuido leve o descuido ligero, que consiste en la falta de aquella diligencia y cuidado que los hombres emplean ordinariamente en sus propios negocios. Esta especie de culpa se atribuye a quien debe administrar sus negocios como un buen padre de familia.

Culpa o descuido levísimo, que consiste en la falta de aquella esmerada diligencia que un hombre juicioso emplea en la administración de sus negocios importantes.

Esta clasificación resulta importante, en la medida en que el artículo 989 del Código Civil, da lugar a que se asignen diversos tipos de culpa según el tipo de contrato y tomando en cuanta que las partes pudiesen pactar la renuncia a la acción para hacer efectiva alguna de estas especies de culpa. Antes esto último, debe advertirse que por

disposición del propio Código en el artículo 987, tratándose de culpa grave o dolo, estos pactos resultarían nulos. Por su parte tratándose de las otras especies de culpa, tales pactos podrían dar lugar a que los tribunales moderaran el grado de responsabilidad, según dispone el artículo 988 del Código Civil.

A diferencia de lo anterior, en materia de responsabilidad extracontractual, se responde de todo tipo de culpa, tal y como se infiere de lo que establece el artículo 988 del Código Civil.

3. En cuanto a la Solidaridad.

En materia de responsabilidad contractual, en el ámbito civil, no existe solidaridad entre deudores, salvo pacto en contrario, por lo que se presume la responsabilidad mancomunada, tal y como lo evidencian claramente los artículos 1024 y 1025 del Código Civil. Por su parte, tratándose de responsabilidad extracontractual resulta lo contrario, es decir, siempre se presumirá la solidaridad entre los deudores, pues así lo expresa el artículo 1644 el Código Civil.

4. En materia de carga de la prueba.

Si la responsabilidad es contractual, la culpa se presumirá como existente desde el momento en que el deudor incumpla, de tal forma que corresponderá a éste probar su no responsabilidad y al acreedor únicamente probar la existencia del título y del incumplimiento. En cuanto a la responsabilidad extracontractual, será la víctima quien

tendrá la carga de probar la culpa del causante o autor del hecho dañoso. No obstante esto último, cabe advertir que en algunos casos se incorporan normas a la legislación positiva con la finalidad de establecer presunciones de culpa en contra del causante o autor del hecho dañoso, como en el caso de la responsabilidad que para el constructor sobreviene conforme a la artículo 1649 del Código Civil.

5. En razón de la extensión del resarcimiento.

Tratándose de responsabilidad contractual, el artículo 992 del Código Civil establece que el deudor de buena fe, sólo responde de los daños y perjuicios, que hubiesen sido previstos o que se hayan podido prever al tiempo de constituirse la obligación y que sean consecuencia necesaria del incumplimiento. Esto, salvo el caso de dolo, pues ante éste se responderá de todos los daños y perjuicios que conocidamente se deriven de la falta de cumplimiento de la obligación. Siendo la responsabilidad extracontractual, el autor del daño responderá siempre conforme a esta última regla.

6. En materia de mora.

De ser la responsabilidad contractual, resultará necesario que el deudor incurra en mora, para lo cual se requerirá que el acreedor le exija judicial o extrajudicialmente el cumplimiento de la obligación, lo que también se conoce como interpelación o intimación. Sin embargo, por disponerlo así el artículo 985 del Código Civil , la misma no será necesaria en varios casos, a saber: si el deudor no ha cumplido sus obligaciones

en el tiempo pactado; cuando la propia obligación o la ley, hagan esta formalidad innecesaria; o, cuando la naturaleza y circunstancias de la mora hayan determinado, que la época de cumplimiento de la obligación ha sido un elemento fundamental para la constitución de dicha obligación.

Tratándose de responsabilidad extracontractual, las obligaciones dimanantes deben cumplirse de forma inmediata, sin que el factor mora tenga ninguna incidencia.

7. En cuanto a la atenuación de la responsabilidad.

En materia de responsabilidad contractual, las partes no pueden invocar el principio de libertad contractual en todos los casos, para los efectos de atenuar su responsabilidad. Ello es así por cuanto el propio Código Civil, en su artículo 987, establece la nulidad de toda cláusula que implique una renuncia a la acción para hacer efectiva la misma, cuando ésta tuviese su origen en el dolo. Por otra parte y como ya lo dejamos sentado, aquella que proviniese de la culpa es sólo moderable por los tribunales (artículo 988). Por ello, tan sólo fuera de estos casos, podría aceptarse el hecho de que las partes atenuasen su responsabilidad en un contrato.

A diferencia de lo anterior, estando frente a una responsabilidad civil extracontractual, no existe ninguna posibilidad de que las partes lleguen a ningún acuerdo sobre el grado de la responsabilidad dimanante del hecho dañoso. Bajo estas circunstancias no resulta viable ningún pacto que de alguna forma atenúe la responsabilidad.

8. En cuanto a la prescripción.

En este aspecto tan poco hay uniformidad, puesto que en lo contractual, los términos de prescripción varían dependiendo del contrato de que se trate, aunque la prescripción general se fija en siete años (artículo 1701 del Código Civil). En materia extracontractual el término de prescripción es único y lo fija la ley en un año (artículo 1706 del Código Civil).

D. Sub-divisiones en la Responsabilidad Civil Contractual y en la Extracontractual.

La responsabilidad contractual puede dividirse según la carga de la prueba (Tamayo Jaramillo, 1986: 9) en obligaciones de medios y obligaciones de resultado, clasificación ésta que como veremos (Infra, pág. 33) cobra mucha mayor relevancia tratándose de la responsabilidad profesional. Conforme a esta clasificación, en las obligaciones de resultado, también llamadas determinadas, el incumplimiento del deudor hará presumir su responsabilidad por lo que tocará a éste la carga de probar que no es culpable. Mientras que en las obligaciones de medios, corresponderá al acreedor, en todo caso, la carga de probar la culpa del deudor y su consecuente responsabilidad.

Por su parte, la responsabilidad extracontractual suele dividirse en: responsabilidad directa, también denominada por el hecho propio, responsabilidad indirecta o por el hecho ajeno y responsabilidad por el hecho de las cosas, por el hecho de los animales y por el hecho de las actividades peligrosas.

E. Elementos Comunes.

Ahora bien, ambos sistemas de responsabilidad, tanto el contractual como el extracontractual presentan una serie de elementos comunes, tales como: la antijuridicidad, el daño, la relación de causalidad entre el daño y el hecho y los denominados factores de imputabilidad o atribución legal de la responsabilidad. Veamos someramente en que consiste cada uno de ellos.

1. La antijuridicidad.

La antijuridicidad implica el actuar en contra de los preceptos de la Ley, incluyendo en lo civil, el incumplimiento de las disposiciones contractuales que para las partes son ley (artículo 976 del Código Civil). Santos Briz lo expresa así: "si la palabra ley se toma en sentido lato incluyendo los pactos contractuales, que son ley para los contratantes, puede llegarse a un concepto aceptable de antijuridicidad" (Bustamante Alsina, 1993:105).

2. El daño.

El daño implica ante todo un desbordamiento de la propia órbita de facultades y una invasión de la ajena (Ibidem, pág. 157). Es la lesión que se causa a un bien jurídicamente protegido o el interés legal de una persona ajena, tomando en cuenta que si tal bien forma parte del patrimonio de esa persona, estaremos en presencia de una

daño patrimonial. Realmente, en lo que se refiere a la clasificación del daño, se hace alusión al daño patrimonial o extrapatrimonial, dependiendo más que nada a la naturaleza del interés legítimo que resulta lesionado en un momento dado, sea este patrimonial o extrapatrimonial.

Por otra parte, la doctrina ha distinguido entre daño patrimonial directo, o sea aquel "que ha inferido inmediatamente un menoscabo o perjuicio en el patrimonio de la víctima, es decir, en sus bienes" (Zannoni, 1993:121). y daño patrimonial indirecto, es decir: "el daño que se ha inferido a bienes jurídicos extrapatrimoniales de la víctima, es decir, a los llamados derechos de la personalidad -su integridad física, el honor, la intimidad, la propia imagen, etc.- que, sin embargo, en forma mediata se traducen en perjuicios o pérdidas patrimoniales" (Ibidem). También se señala que existe daño directo cuando quien lo sufre es la víctima directa del hecho e indirecto cuando el mismo afecta a personas distintas de aquél (*dommage par ricochet ou réflechi*).

Otra clasificación es la que hace alusión a la lesión de un interés positivo, como cuando se incumple un contrato válido, toda vez que se tenía un interés en el cumplimiento del mismo. Este tipo de daño se constituye por la diferencia patrimonial ocasionada por la inexistencia o demora de la prestación, o sea el incumplimiento; mientras tanto el interés negativo es la diferencia patrimonial entre la situación actual y la situación patrimonial que se hubiese dado si la eficacia de la obligación no se hubiese frustrado (*pérdida de un chance*) (Parellada, 1990: 62).

El daño también tiene algunos requisitos tales como:

El de ser cierto, es decir que el mismo exista actualmente o que su existencia sea probable. Esta certeza puede ser mayor o menor, por lo que la misma se refleja en diferentes supuestos que en grado de menor a mayor son: la chance, la cual se ubica en un grado intermedio entre lo que es hipotético y lo que es probable. En este sentido se

dice que hay *pérdida de un chance,* cuando ha habido una ruptura en el proceso que podía conducir a la obtención de una ganancia o el evitar un daño (Parrellada, 1990:47). El lucro cesante, que se acerca más a la certeza del daño, consiste en la privación de una ganancia esperada que se basa en una probabilidad específica. El daño emergente, que es un daño completamente revestido de certeza, es decir el que se ha realizado o que se realizará como consecuencia de la lesión sufrida por la víctima. Pero también es indemnizable el daño futuro, que es aquel que será una consecuencia necesaria del daño inferido.

Debe existir un interés personal del accionante, porque quien reclama el daño debe ser el que lo ha sufrido.

Ser subsistente al momento de la sentencia, pues el daño no debe haber sido reparado por el victimario o un tercero, ya que de haberlo sido, no habrá objeto para la acción que se haya incoado contra el responsable del mismo.

3. La relación de causalidad.

La relación de causalidad entre el daño y el hecho determina que aquel daño que requiere ser reparado, debe tener una relación causal adecuada con el hecho de la persona o la cosa a las que se les atribuye dicho daño. Este "nexo de causalidad" (Parellada, 1990: 261) resulta esencial para no incurrir en la falta de atribuir el daño a una persona o cosa distinta de aquella que realmente lo causó. Sin embargo, para aclarar el alcance de este elemento fundamental de la responsabilidad civil, resulta necesario mencionar que tal relación de causalidad puede verse rota o interrumpida, en la medida en que se presenten situaciones tales como la culpa de la propia víctima en la

producción del daño, la existencia de caso fortuito o fuerza mayor y cuando el hecho dañoso es atribuible a un tercero diferente del presunto causante del daño.

4. Factores de imputabilidad.

La Ley debe establecer aquellos factores (llamados de imputabilidad) en base a los cuales se determinará si una persona es o no es civilmente responsable. Es decir si se le puede atribuir o imputar dicha responsabilidad. Estos factores pueden ser de carácter subjetivo, y así tenemos al dolo y la culpa, u objetivos, entre los cuales podríamos destacar: el riesgo, la garantía, la equidad, el abuso del derecho y el exceso de la normal tolerancia.

(a). Factores subjetivos de imputabilidad.

En relación con lo mencionados factores de responsabilidad, hemos de señalar que el factor subjetivo resulta ser el preponderante no solo en nuestro derecho, sino que también a nivel del derecho comparado. En nuestra Legislación, los artículos 986 y 989 del Código Civil, reflejan la necesaria presencia de este factor en materia contractual. Por su parte el artículo 1644 y siguientes de dicho Código, sustentan la esencial existencia del factor culpa tratándose de responsabilidad extracontractual. Estas disposiciones no dejan lugar a duda sobre la necesidad de que el actuar del supuesto causante del daño deba ser de carácter doloso o culposo, pues de lo contrario y salvo la

existencia de una norma que señale lo contrario, no le sería atribuible responsabilidad alguna.

Lo anterior nos lleva a la lógica conclusión de que la existencia de factores ajenos a la culpa, es decir factores objetivos de responsabilidad, dependen, en todo caso, de una Ley que expresamente les de vigencia, ya que en caso contrario se requeriría la presencia del factor culpa como elemento *sine qua non.*

Consideramos necesario en este momento, establecer las principales distinciones conceptuales entre el dolo y la culpa, como factores subjetivos de responsabilidad. Es así que el dolo implica una conducta intencional de causar un daño, o como diría Bustamante Alsina (Bustamante Alsina, 1993: 326), el incumplimiento intencional de una obligación aun estando el deudor en capacidad de hacerlo. La culpa por el contrario, entraña una conducta carente de intensión, pero en la cual el agente omite aquel hacer o no hacer con el cual hubiese previsto o aun evitado el daño.

(b). Factores objetivos de imputabilidad.

En lo que atañe a los principales factores objetivos de responsabilidad, reseñaremos brevemente aquellos a los que principalmente hace alusión la doctrina y nuestro derecho positivo y comparado.

1. El factor riesgo tiene su principal ámbito de aplicación tratándose de los daños ocasionados por cosas inanimadas y por animales. En estos casos se suele establecer que la responsabilidad del daño causado será atribuible a quien tenga bajo su cargo la cosa o el animal de que se trate. El artículo 1647 del Código Civil a propósito del daño causado por animales establece:

> El poseedor de un animal, o el que se sirve de él, es responsable de los perjuicios que causare, aunque se le escape o extravíe. Sólo cesará esta responsabilidad en el caso de que el daño proviniera de fuerza mayor o de culpa del que lo hubiese sufrido.

Por su parte, tratándose del daño causado por las cosas inanimadas, el artículo 1652 del Código reza así:

> El cabeza de familia que habita una casa o parte de ella es responsable de los daños causados por las cosas que se arrojen o cayeren de la misma.

También resulta importante citar el artículo 1650, el cual señala:

> Igualmente responderán los propietarios de los daños causados:
> 1. Por la explosión de máquinas que no hubiesen sido cuidadas con la debida diligencia y la inflamación de sustancias explosivas que no estuvieran colocadas en lugar seguro y adecuado;
> 2. Por los humos excesivos, que sean nocivos a las personas o a las propiedades;
> 3. Por la caída de arboles colocados en sitio de tránsito, cuando no sea ocasionada por fuerza mayor;
> 4. Por las emanaciones de cloacas o depósitos de materias infectantes, construidos sin las precauciones adecuadas al lugar en que estuviesen.

2. El factor garantía tiene su ámbito de aplicación sobre todo en la denominada responsabilidad civil indirecta, siendo la misma aquella que se imputa al principal por los daños causados por los dependientes de éste. A estos efectos el artículo 1645 del Código Civil es claro al señalar:

> La obligación que impone el artículo 1644 es exigible no sólo por los actos u omisiones propios, sino por los de aquellas personas de quienes se debe responder.
> El padre y la madre son responsables solidariamente de los perjuicios causados por los hijos menores o incapacitados que están bajo su autoridad y habitan en su compañía.
> Lo son igualmente los dueños o directores de un establecimiento o empresa respecto de los perjuicios causados por sus dependientes en el servicio de los ramos

> en que los tuvieran empleados, o con ocasión de sus funciones.
> El Estado, las instituciones descentralizadas del Estado y el Municipio son responsables cuando el daño es causado por conducto del funcionario a quien propiamente corresponda la gestión practicada, dentro del ejercicio de sus funciones.
> Son, por último, responsables los maestros o directores de artes y oficios respecto a los perjuicios causados por sus alumnos o aprendices, mientras permanezcan bajo su custodia.
> La responsabilidad de que trata este artículo cesará cuando las personas de derecho privado en él mencionadas prueben que emplearon toda la diligencia de un buen padre de familia para prevenir el daño.

3. Conforme al factor equidad, quien causa un daño sin que mediare voluntad, inclusive por no estar en capacidad de discernir, sólo estará obligado a reparar el daño causado en igual proporción a su enriquesimiento o al incremento que en su patrimonio se causó a consecuencia de referido daño. El artículo 1643 a del Código Civil, al referirse al enriquesimiento sin causa señala:

> Quien se ha enriquecido sin causa, a costa o con perjuicio de otro, está obligado , dentro de los límites del enriquesimiento, a indemnizar a éste de su correlativa disminución patrimonial.

A su vez el artículo 1643 b, señala que la mencionada acción no podrá ejercitarse cuando el perjudicado tenga otra acción para lograr una indemnización por el perjuicio causado. Y en el caso que nos ocupa, si se tratare de un inimputable, es decir, quien carece de discernimiento, pareciese que esta fuese la única forma de lograr la reparación del daño causado, a la luz de nuestra legislación.

4. Finalmente, el factor abuso del derecho implica el ejercicio de un derecho para una finalidad distinta de aquella definida por la *mens legis* o intensión del legislador, causando de tal forma un daño a otro, cuando tal ejercicio contraríe la moral y las buenas costumbres o rebasen los límites de la buena fe. Como señala Mazeud

Tunc: "el que ejercita un derecho con el deseo de causar un daño incurre en una culpa delictual; el que, sin intención maliciosa, se comporta, al ejercitar un derecho, de modo distinto del que lo habría hecho un individuo cuidadoso, con imprudencia o negligencia, incurre en una culpa cuasidelictual; en ambos casos, su responsabilidad es exigible" [1] (Mazeud et al. 1977: 233).

Todos estos factores tienen en común, el hecho de que el causante del daño no queda obligado a reparar el daño en virtud de haber actuado con culpa, sino en virtud de que así lo ha dispuesto la ley.

F. La Responsabilidad Profesional.

Finalmente, queremos hacer mención del concepto de responsabilidad profesional, la cual deviene como una responsabilidad especial, que al decir de Trigo Represas es: "aquella en la que incurre una persona que ejerce una profesión, al faltar a los deberes especiales que ella le impone; se trata, pues, de una infracción típica, concerniente a ciertos deberes propios de esa determinada actividad..." (Trigo, 1987: 27). Y es que pareciese que todo profesional debe poseer los conocimientos teóricos y prácticos propios de su profesión, de tal forma que su obrar se haga con la previsión y diligencia necesarias conforme a las reglas y métodos pertinentes (Ibidem). Aquel profesional que no obra según estos preceptos incurre en la denominada culpa profesional.

Muchos tratadistas hacen una distinción entre la responsabilidad que surge para el profesional al faltar a las reglas de prudencia que se imponen a cualquier persona, lo cual se rige por el derecho común y obliga a la reparación indistintamente de la clase de

culpa de que se trate; y, la que surge por infracción de las reglas de carácter científico que ordenan la profesión, en cuyo caso estamos frente a la culpa profesional y sólo obligan a responder, tratándose de culpa lata o grave. Sin embargo, esta teoría no es unánimemente aceptada, criticándosele su inaplicabilidad en la mayoría de los casos y el hecho de que los profesionales no sólo deben responder por culpa grave, si aceptamos como bueno el principio de imputabilidad de las culpas y la reparación de todo daño causado, ya sea por el hecho propio o por la propia negligencia o imprudencia. Un fallo de la Corte de Casación Francesa del 21 de julio de 1862, sostuvo este principio, pero añadió que la responsabilidad profesional se ajusta al derecho común, siempre y cuando el tribunal pueda probar sin lugar a dudas, es decir sin entrar a discurrir en materias que sólo los especialistas comprenden, una culpa cometida por un profesional, indistintamente de su gravedad, procediendo en tal caso a condenar al profesional a reparar los daños causados (Trigo, 1987: 30 a 32).

Ahora bien, la determinación de la culpa profesional debe prescindir el recurrir al clásico actuar del buen padre de familia, es decir el actuar del hombre promedio y fundamentarse en el estereotipo del buen profesional, del hombre dotado de conocimientos o aptitudes de nivel superior. Pero este deber del profesional de prestar sus servicios sobre la base de esos conocimientos o aptitudes de nivel superior, de los cuales esta dotado, realizando su labor con prudencia y diligencia y atento a las circunstancias de las personas, del tiempo y del lugar, hace que se concluya que sus obligaciones deban ser casi siempre de medios y no de resultados. Esta última distinción, atribuida a Demogue, determina que las obligaciones de medios son aquellas en virtud de las cuales el obligado no garantiza el resultado de su labor, sino únicamente la disposición del mismo para intentar obtener este resultado con un actuar diligente y apto, tal sería el caso de las obligaciones de médicos y abogados; mientras que las

obligaciones de resultado son las que garantizan la consecución de un resultado determinado en todo caso, como aquellas que contraen los ingenieros y arquitectos (Trigo, 1987: 34 a 35).

Sin embargo, cabe advertir que no puede afirmarse que toda obligación profesional siempre será de medios o de resultados, pues todo dependerá del profesional de que se trate y de la labor que realice el mismo. En todo caso, la responsabilidad profesional surgirá siempre que el profesional actúe apartado de los preceptos que rigen su ciencia o con inaptitud para el ejercicio de la misma.

La responsabilidad profesional puede ser contractual o extracontractual. Sin embargo, la relación con sus clientes al estar siempre fundamentada en un contrato de prestación de servicios profesionales será contractual. Incluyendo esta última, obligaciones de medios o de resultados. La responsabilidad profesional extracontractual surgirá en los casos en los cuales los profesionales en el ejercicio de su profesión, causen daños a terceros o cuando causen daño a aquella persona a la cual presten sus servicios sin que medie ningún contrato, como en la gestión de negocios ajenos o cuando la misma resulta de un imperativo ético o legal.

Del actuar de los profesionales se derivan una serie de obligaciones especiales tales como: las obligaciones de corrección y buena fe, las cuales incluyen el deber de mantener en todo momento informado al cliente sobre el curso de sus negocios; el deber de consejo sobre las cuestiones propias de los servicios que se le prestan; y, el actuar con fidelidad y corrección en la prestación del servicio profesional. El Profesor Del Moral (Del Moral, 1993a), citando al autor italiano Cattaneo, advierte la existencia de una clasificación de estas obligaciones en integrativas instrumentales, entre las cuales se incluyen los deberes de fidelidad, de conocimiento científico o actualización científica y el deber de información al cliente; y, por otra parte, las obligaciones de protección y

corrección, entre las cuales destacan los deberes de no retener documentos, de no perjudicar al cliente luego de resuelta la relación contractual profesional y el secreto profesional.

II. Consideraciones Generales sobre la Responsabilidad Civil de los bancos.

A. Naturaleza de la Responsabilidad.

Los bancos, en el ejercicio de la actividad que les esta legalmente autorizada, son susceptibles de lesionar o agraviar bienes jurídicos o intereses legales de sus clientes, con lo cual quedan sometidos al régimen legal de la responsabilidad civil y asumen la obligación de reparar los daños causados por el actuar dañoso. Como señala Mazeud Tunc: "El banquero, como cualquier otro profesional, responde contractualmente ante sus clientes (...) por sus culpas, incluso leves" (Mazeud, 1977: 193). Esta responsabilidad, según Mazeud Tunc, debe resolverse por la aplicación de los principios generales de la culpa.

En términos generales, la responsabilidad civil de los bancos es de carácter contractual como señala Mazeud Tunc, pues la relación de éste con sus clientes se fundamenta en todo caso en un contrato que, al decir de Rodríguez Azuero (Rodríguez Azuero, 1990: 116), antecede la realización de una operación bancaria. Estos contratos pueden tener por objeto la realización de las llamadas operaciones activas, en cuyo caso la responsabilidad sobrevendría para el banco, por el incumplimiento de sus obligaciones para con los receptores de los bienes de capital que el banco recibe para

invertir por su cuenta y riesgo. La responsabilidad del banco que otorga un crédito, a cobrado importancia sobre todo en la jurisprudencia foránea y especialmente en los Estados Unidos de América. Algunos casos específicos son mencionados por Bollini Shaw y Boneo Villegas (Bollini Shaw et al., 1990: 249), entre estos tenemos: el banco que fue condenado por procesar equivocadamente la información proporcionada por los clientes y haber otorgado menos dinero del acordado, a pesar de que la obligación estaba debidamente garantizada (Jackes vs First Nat. Bank of Maryland); por igual falta se condena a otro banco en el caso Commercial Standart Insurance Co. vs Bank of America, 1976 y Davis vs Nevada Nat. Bank, 1987. En otras situaciones, algunos bancos han resultado condenados por suspender o cancelar definitivamente una línea de crédito sin previo aviso, lo cual se considera un acto de mala fe o falta de *fear dealing*, o lo que en nuestro medio podríamos considerar un acto doloso. Tal actuación se suscitó en el caso de KMC Co. Inc. vs Irving Trust Co., 1987. Otros bancos han sido condenados por daños en la gerencia de negocios ajenos, lo cual ocurre cuando el banco recomienda la designación de determinados o todos los directores o gerentes de una empresa de la cual es acreedora y tales dignatarios o empleados actúan de forma negligente, ocasionando un severo daño financiero a dicha empresa. En los casos: State National Bank of El Paso vs Farah Manufacturing Co. Inc. (1984) y American Lumber Co. vs Trust Nat. Bank of St. Paul (1989), un banco fue condenado al pago de 18,5 millones de dólares por esa causa.

Consideramos relevante también advertir la responsabilidad en que incurre el banco cuando habiendo prometido el otorgamiento de un crédito, no cumple con su ofrecimiento. Para algunos en esta fase podría no haber un contrato, sin embargo olvidan que habiendo una manifestación clara de obligarse por parte del banco y de aceptar el crédito por parte del cliente, se perfecciona al menos un contrato de promesa,

cuyo incumplimiento genera responsabilidad para las partes. Así la jurisprudencia estadounidense ha establecido que al acordar un banco con su cliente el otorgamiento de un préstamo, el banco no puede requerir nuevas condiciones, ni retrasar su entrega o aún renegociar el mismo, tal y como se sentenció en el caso de Penthouse International Inc. vs Dominion Federal Savings &. Loan Asociation.

Bollini Shaw y Boneo Villegas (Bollini Shaw et al., 1990: 250) asignan al banco algunas otras obligaciones contractuales dentro de su análisis de la casuística bancaria, así tenemos: el deber de informar a su cliente, la obligación de otorgar el crédito de forma razonable, de buena fe y justamente; el deber de no tolerar un incumplimiento reiterado de su cliente de los términos de un contrato bancario, pues el cliente puede considerar que tal conducta ha sido aceptada por el banco como convenida; el banco tiene el deber de notificar a su clientela la terminación del contrato de crédito con antelación.

Pero también el objeto puede ser el de las llamadas obligaciones pasivas, en cuyo caso el banco incurre en responsabilidad si incumple las obligaciones contraídas con aquellos que le proveen de los bienes de capital que fundamentalmente, le permiten a éste el ejercicio de su actividad intermediadora, como veremos más adelante.

Finalmente se acepta la existencia de las llamadas operaciones neutras, en las cuales el banco no realiza una operación propiamente de intermediación en el crédito, sino más bien brinda un servicio específico.

Los contratos bancarios pueden incluir las llamadas obligaciones de medios, para los casos en los cuales el banco no se obliga a obtener un resultado específico, sino a emplear la mayor diligencia posible en obtenerlo, siendo el caso que la responsabilidad del mismo sobrevendrá, por el hecho de que el cliente compruebe la culpabilidad del banco ante el daño causado. El banco asume obligaciones de medios cuando su deber

consiste en disponer de bienes de su cliente para un fin específico, pero asumiendo el cliente el riesgo. Tal es el caso de los contratos que anteceden algunas operaciones de carácter bursátil o en los cuales la especulación es uno de los principales elementos. En estos casos el banco puede obligarse ya sea a: comprar o vender títulos cotizables en una bolsa de valores, no obstante lo cual el cliente asume el riesgo resultante de los réditos o las pérdidas que se obtengan durante las operaciones pertinentes; el banco también puede comprometerse con su cliente a emitir y colocar por su cuenta y riesgo, un número determinado de títulos de obligación o suscribir los mismos, pero igualmente sin responsabilidad para el banco; y, también puede el banco actuar como fiduciario en la emisión de títulos de obligación para los efectos de administrar los mismos por cuenta y riesgo del fideicomiso. También pueden considerarse como obligaciones de medios, ciertos contratos en los cuales el banco actúa como intermediario en los pagos o en los cobros, los cuales realiza por cuenta de su cliente. Y en términos generales en aquellos contratos cuyo objeto es la realización de un mandato en los cuales el banco sólo asume responsabilidad por la diligencia con la cual cumple su encargo.

Por su parte, el banco asume obligaciones de resultado en la mayor parte de sus operaciones, pues en éstas se compromete no sólo a actuar sobre la base de su supuesta competencia y capacidad, sino que garantiza el fin del contrato y reconoce en el incumplimiento su culpa, razón por la cual le corresponderá la carga de probar la existencia de una causa extraña (Tamayo, 1986: 9) como única fórmula liberadora. Por ello, en los contratos que anteceden operaciones pasivas, el banco garantiza la devolución con intereses del dinero en efectivo que es depositado en éste por sus clientes, como en el caso del contrato de depósito en cuenta de ahorros, a plazo o a la vista, aunque vale la pena advertir que conforme a la legislación panameña, en este último caso no se pagan intereses; por su parte en los contratos que anteceden las

operaciones activas, el banco puede comprometerse, entre otras cosas, a mantener una determinada suma de dinero o una facilidad crediticia a disponibilidad de su cliente, tal es el caso de las distintas aperturas de crédito, aunque también puede el banco obligarse a otorgar un crédito a cambio de una garantía previamente constituida como en el anticipo bancario o aún a adelantar el nominal de un título de crédito menos una suma de dinero que ingresa como ganancia del banco y que suele denominarse como tasa de descuento, en el denominado descuento de títulos.

También suelen asumirse obligaciones de resultado, en los contratos que anteceden la realización de las operaciones denominadas neutras, tales como: las transferencias bancarias, los giros y el arrendamiento de cajillas.

Por otra parte, la responsabilidad de los bancos puede ser igualmente extracontractual, en la medida en la que dentro del ejercicio de su actividad, afecte los bienes o intereses jurídicos de terceros. Esto último ocurre generalmente cuando los bancos se ven en la necesidad de intercambiar información sobre sus clientes, ya sea para considerar la apertura de un depósito o de un crédito o a requerimiento de un tercero, cuando el cliente así lo autoriza o una autoridad competente así lo requiere. En estos casos el banco deberá tener el cuidado de que la información que brinde sea correcta y precisa, toda vez que en caso contrario, puede afectar los bienes o intereses de otros bancos, entidades financieras o de cualquier otro tercero que recibe dicha información, dado el caso que la misma resulte incorrecta, y ésta incida ya sea en la apertura de una cuenta de depósito utilizada para fines ilícitos, la concesión de un crédito a una persona insolvente o que resulte en que un tercero se cree una falsa imagen del cliente del banco y actuando en consecuencia resulte perjudicado.

Bollini Shaw y Boneo Villegas (Bollini y Boneo, 1990: 250) mencionan dos casos sobre información errónea proporcionada por una banco que causó daños a terceros.

Así tenemos, el caso de Central States Stamping Co. vs Terminal Equipment (1984), en el cual un banco que era acreedor principal y manejaba el gasto diario de una empresa subcapitalizada, informa a un comprador de equipos que la empresa tenía referencias satisfactorias, a sabiendas de su estado financiero. Siendo ello así, el comprador adelantó a la empresa cincuenta mil dólares, los cuales fueron parcialmente entregados al banco y parcialmente malgastados. A consecuencia de la imposibilidad de la empresa de devolver el dinero, ésta fue a la quiebra. El banco fue condenado a pagar al referido comprador, los cincuenta mil dólares que se habían adelantado a la empresa quebrada. El banco fue declarado responsable por cuanto éste conocía las condiciones de la empresa deudora.

Otro ejemplo es el de Bank of New Richmond vs Production Credit Association. En este caso, una entidad crediticia que es acreedora mayoritaria de un granjero promueve el otorgamiento de créditos a dicho granjero, hasta el punto de que este último queda insolvente y sin capacidad para pagar. Ante tal hecho, un banco demanda a la entidad crediticia que promovió el otorgamiento de los créditos y ésta es condenada, al dictaminarse que existía un *joint venture* o asociación de hecho entre la entidad y el granjero, debiendo la entidad responder como garante de las obligaciones del granjero.

La jurisprudencia estadounidense ha llegado inclusive a condenar a un banco que continuamente financiaba la labor de un granjero y que al no renovarle los créditos, llevó a este último a la quiebra (Bollini y Boneo, 1990: 250).

Mazeud Tunc (Mazeud, 1977: 193 a 196), nos brinda una numerosa cantidad de casos en los cuales los bancos son responsables, entre ellos tenemos: el pago de cheques falsos o cobrados por tenedores fraudulentos; la negativa del banco a pagar cheques regulares y cubiertos con provisión de fondos suficientes; las indicaciones erróneas o insuficientes suministradas acerca de los valores, sobre los clientes o sobre

terceros; por órdenes de bolsa inexactamente transmitidas; por el olvido de prevenir a los depositantes algunas operaciones que habían de realizarse con los títulos depositados o la pérdida de esos títulos; por errores en los pagos; por débitos abusivos; por retraso en los giros pendientes, en los cobros que hayan de hacerse o incluso en las medidas ejecutivas que hayan de tomarse contra el cliente; por el hecho de no haberle indicado al librador de una letra de cambio la falta de pago de esa letra; o al beneficiario de un cheque, la falta de provisión de fondos suficiente para cubrir ese cheque; por la pérdida en el curso de la expedición, de títulos al portador o de efectos a la orden; por la pérdida o el deterioro de los objetos depositados en cajas de seguridad; por la obediencia a una orden judicial de discutible aplicación.

La responsabilidad extracontractual del banco, siendo este por regla general una sociedad anónima, puede ser directa o por el hecho propio, cuando éste actúa a través de sus organismos directivos (Junta Directiva o Junta de Accionistas), o indirecta o por el hecho ajeno, toda vez que los actos delictivos o cuasidelictivos que causan un daño a un bien o interés jurídico de un cliente, pueden también ser causados por los empleados del banco, quienes entran en la categoría de dependientes de aquél, conforme a lo previsto por el artículo 1645 del Código Civil. En estos casos la culpa puede ser *in eligiendo* o *in vigilando*, ya sea que se atribuya al banco una falta en sus procedimientos de contratación de personal o que se le atribuya una falta de cuidado o control sobre sus empleados. Si el banco tuviese naturaleza oficial, o sea un ente de derecho público, entonces el banco será responsable de forma indirecta, siempre que el funcionario que causó el daño sea aquel a quien propiamente corresponda la gestión practicada. Sin embargo, el párrafo final del artículo 1645, antes mencionado, señala que si la entidad fuese de derecho privado, esta puede liberarse de responsabilidad, siempre y cuando logre probar que empleo toda la diligencia de un buen padre de

familia para prevenir el daño. No obstante consideramos que para que esta disposición puede aplicarse a la banca privada, se requeriría la prueba de que se actuó como lo demanda un buen profesional de la banca, toda vez que la responsabilidad de los bancos no puede definirse sino como una responsabilidad profesional (Supra, pág. 32).

B. Bienes e intereses jurídicos susceptibles de daño por el actuar del banco.

La responsabilidad civil de los bancos puede implicar la lesión de diversos bienes jurídicos tanto de naturaleza tangible, como es el caso de los dineros, títulos valores, bienes inmuebles u otros que el cliente confíe al banco, ya sea en depósito, en administración, en fideicomiso, en garantía o bajo cualquier otra fórmula que implique para el banco el recibir la propiedad o al menos la posesión de parte del patrimonio de su cliente; pero también de naturaleza intangible, como es el caso de aquellos afectados por el denominado daño moral, el cual es previsto por nuestra legislación en el artículo 1644a del Código Civil. En este último caso y conforme a la descripción legislativa, podrían lesionarse intereses extrapatrimoniales vinculados con bienes tales como: el decoro, el honor, la reputación, la vida privada o intimidad, entre otros. Inclusive puede el banco afectar un interés jurídico de su cliente cuando de alguna manera priva a éste de la facultad o poder de disfrute o disposición de uno de los mencionados bienes jurídicos. Ello es así cuando el banco niega a su cliente el acceso a su cuenta bancaria o cuando le interrumpe el derecho a recibir los dineros u otros bienes de capital a los que tiene derecho en virtud de una apertura o línea de crédito celebrada con éste.

Cabe aclarar que el daño moral, al cual hemos hecho alusión, debe diferenciarse del denominado daño patrimonial indirecto al que hicimos referencia anteriormente

(Supra, pág. 25), toda vez que el primero implica la lesión o menoscabo de intereses extrapatrimoniales en razón de un evento dañoso y a la vez antijurídico, mientras que el segundo si bien implica en principio la lesión a un derecho sobre un bien jurídico extrapatrimonial, en definitiva derivará en el hecho de que la víctima sufrirá un menoscabo en un interés patrimonial. Debe tenerse claro que la diferencia entre daño patrimonial o extrapatrimonial radica en el interés lesionado y no en el bien jurídico afectado.

III. La actividad bancaria como determinante de la responsabilidad civil de los bancos.

La actividad bancaria o negocio de banca podría ser definida, en términos sencillos, como aquella en virtud de la cual ciertas entidades ejercen una función intermediadora del crédito, que consiste en tomar bienes de capital del público principalmente bajo la forma de depósitos y luego invertir tales bienes en forma pública, bajo distintas modalidades entre ellas el préstamo y la apertura de crédito. El Decreto de Gabinete 238 de 2 de julio de 1970, por el cual se reforma el régimen bancario y se crea la Comisión Bancaria Nacional, por su parte, define el negocio de banca en su artículo dos, literal b, así:

> Principalmente la operación de captar recursos financieros del público por medio de la aceptación en depósito de dinero exigible a la vista o a plazo o por cualquier otro medio autorizado por la ley al efecto; y la utilización, por cuenta y riesgo del banco, de tales recursos para préstamos, inversiones o cualquier otra operación autorizada por la ley o los usos bancarios;
>
> .....

Ahora bien, si quisiésemos plasmar una definición de actividad bancaria que tratara de reunir todos los elementos que caracterizan a este negocio, tendríamos que afirmar que la actividad bancaria es aquella que realiza la empresa mercantil que como parte de un sistema presta un servicio público, de forma masiva y a través de la fórmula de la intermediación financiera, asumiendo los riesgos que resulten y con una cuidadosa reserva de la información que obtengan de sus clientes frente a terceros.

De las definiciones anteriores podemos extraer una serie de elementos que son comunes y que de hecho caracterizan a la actividad bancaria, los cuales van a configurar sus peculiaridades, incluyendo la forma en la que deben responder los bancos frente a las obligaciones que contraigan o que surjan para ellas en el ejercicio del negocio. Veamos pues cuales de estos elementos vale la pena resaltar.

A. El carácter comercial o mercantil.

Aunque la mayoría de los autores no lo mencionan por considerarlo algo obvio, la actividad bancaria tiene ante todo un carácter comercial o mercantil. Esto resulta de suma importancia pues va a determinar la naturaleza de la Ley que regule esta actividad. En tal sentido, nuestro Código de Comercio de forma expresa, considera a las operaciones bancarias como actos de comercio y por lo tanto sometidos en todo a la Ley comercial. A este respecto el artículo 1° del Código de Comercio señala:

> La Ley comercial rige los actos de comercio, sean o no comerciantes las personas que en ellos intervengan; y las acciones que de ellos resulten o cualesquiera actos relacionados con los mismos se regularán conforme a lo dispuesto en el Código Judicial.

A su vez el artículo 2° del referido Código en el numeral 6° dispone lo siguiente:

> Serán considerados actos de comercio todos los que se refieren al tráfico mercantil, reputándose desde luego como tales, los contratos y títulos siguientes:
> .....
> 6° El cambio y los demás contratos de que pueden ser objeto el dinero y los títulos que le representen en su calidad de mercancías, comprendidos generalmente bajo la denominación de operaciones de banca.
> .....

Resulta preciso agregar que al calificarse a los bancos como comerciantes , sus contratos y obligaciones se considerarán siempre actos de comercio, a menos que fueren de naturaleza exclusivamente civil, o si no resultare lo contrario del acto mismo, tal y como se infiere del artículo tercero del Código de Comercio. Igualmente, debe tenerse en cuenta que siendo el acto comercial para el banco, se aplicará en todo caso la ley mercantil en cuanto a las consecuencias y efectos de tal acto, como se infiere del artículo cuarto del Código de Comercio. Esto último a pesar de que la contraparte del banco en el negocio de que se trate, no tenga la calidad de comerciante.

B. La intermediación.

La intermediación constituye el elemento comúnmente encontrado en todas y cada una de las definiciones sobre el negocio o actividad bancaria, por constituir el eje central de la misma. Este elemento podría definirse como: la captación de recursos de capital y su transferencia a los sectores productivos de la actividad económica (Rodríguez, 1990: 102). Debemos tomar en cuenta en adición y como una nota jurídicamente trascendente, que la transferencia es efectuada por el transferente asumiendo por su cuenta y riesgo los daños que se originen de dicha actividad y que en

tal caso el banco asume, de principio, una doble responsabilidad civil por los daños que ocasionen en el ejercicio de dicha actividad de intermediación, por una lado con los clientes que le confían sus recursos de capital y por el otro con los clientes que reciben tales recursos, sin perjuicio de los daños que su actividad pueda causar a terceros.

C. La masividad.

Ésta implica la realización de la intermediación bancaria pero en forma continua y en proporciones masivas. Esta característica surge de la teoría de los actos en masa expuesta en 1902, por el jurista alemán Heck, para intentar explicar los efectos de la revolución industrial en el ámbito jurídico, siendo la misma muy relevante para nuestro estudio. Y es que el volumen de las operaciones de los bancos, incide directamente en un aumento cuantitativo del riesgo de lesionar el patrimonio en razón de un error humano de quienes participan en el procesamiento de dichas operaciones o dicho de otra forma, de aquellos funcionarios bancarios que le dan vida a las mismas en el ámbito jurídico y contable, aun cuando algunos autores como Díaz Ramírez manifiesten que:

> La contratación en serie o en masa les permite a los bancos reducir el riesgo que significaría celebrar contratos distintos con cada cliente: la homologación de la contratación equivale para la empresa financiera, ni más ni menos, desde el punto de vista jurídico, a reducir a uno el riesgo de tener vigentes miles de contratos (Díaz, 1983: 3).

Nuestra discrepancia con el mencionado autor consiste en que, en nuestra opinión, la reducción a la que éste alude, no es una reducción propiamente

en los riesgos sino en la dificultad material que implica el efectuar operaciones hechas a la medida de cada cliente.

Los daños que el tratamiento masivo de las operaciones bancarias pueden causar, son susceptibles de lesionar tanto el patrimonio como los derechos intangibles de los clientes, entre ellos la reputación, la imagen y la intimidad. Igualmente incide tal característica de forma directa, en la necesidad que surge para las entidades bancarias de adoptar las fórmula de los contratos de adhesión o *contratos-formulario* (Bonfanti, 1980: 19) y consecuentemente las denominadas *condiciones generales de la contratación bancaria* (Garrigues, 1983: 167), entre las cuales podemos señalar:

1. El hecho de que se autorice u obligue al banco según el caso, a realizar pagos por cuenta del cliente.

2. La obligación del banco de abonar los cheques que el cliente le remita con cargo a su provisión de fondos.

3. El derecho contractual de prenda de que goza el banco para garantizar el pago de sus saldos deudores.

4. El derecho de compensación del banco que rebasa los límites de la compensación legal.

5. La obligación del banco de abonar los intereses a su cliente en las operaciones pasivas y el de adeudarlos en las activas. Teniendo en cuenta que el interés de las operaciones activas es mayor que el de las pasivas y cuya diferencia es el denominado *spread.*

6. El banco percibe en adición a los intereses, un tanto fijo o porcentual denominado comisión, por los servicios que realice por encargo de su cliente.

7. El banco tiene un deber de lealtad y diligencia en relación con los informes y consejos que brinde a su cliente y debe asumir la responsabilidad de carácter profesional por el daño que ocasione por las incorrecciones o faltas que cometa en tales casos.

8. La obligación de reserva de la información, sobre todo en lo referente a la relación contractual que lo une a su cliente.

Estas condiciones generales constituyen para algunos (Bonfanti, 1980: 24), un elemento que reemplaza a los usos bancarios, los cuales han decaído en importancia como fuente de derecho bancario.

Más recientemente la masividad ha ocasionado que los bancos recurran al procesamiento electrónico de la información que reciben de sus clientes, con toda la responsabilidad que esto último conlleva en cuanto a la seguridad de la información que también es depositada en los llamados *bancos de datos* de estas entidades, sobre todo ante la susceptibilidad de estos sistemas a la pérdida, alteración o sustracción no autorizada de la información de los clientes. Situación ésta que trataremos a fondo en los capítulos posteriores de este estudio.

D. La adhesividad contractual.

Esta característica que es una consecuencia de la masividad de que hablábamos en el literal anterior, adquieren, en nuestro concepto, una relevancia tan especial que consideramos adecuado efectuar un análisis aparte y más detallado de la misma.

En Panamá la reciente Ley 29 de 1 de febrero de 1996, define el contrato de adhesión como: "aquel cuyas cláusulas han sido establecidas unilateralmente por el proveedor de bienes y servicios, sin que el consumidor pueda negociar su contenido al momento de contratar". Y es el caso que en la contratación bancaria, es la institución la que impone los términos y condiciones de la relación por regla general, adhiriéndose el cliente a las mismas o sencillamente optando por no contratar con el banco.

Ahora bien, la Ley 29, tiene efectos sobre la contratación bancaria, toda vez que la misma busca proteger a un cliente que como consumidor de los servicios bancarios y financieros que el banco le ofrece, se encuentra en un aparente estado de inferioridad jurídica, dada la antedicha naturaleza adhesiva de esta contratación. Dicho en otras palabras, la Ley busca crear un real equilibrio contractual mediante medidas de protección de los clientes. Así se establecen una serie de obligaciones que los bancos como proveedores de servicios bancarios y financieros deben asumir. De lo dispuesto por el artículo 31 de la Ley 29, hemos inferido las siguientes obligaciones para los bancos:

1. La de informar, clara y verazmente a sus clientes, sobre las características de los servicios ofrecidos.

2. La de indicar, en forma expresa y visible, cuando el servicio que se presta se pague al crédito, como en la mayoria de los servicios bancarios, sobre todo los que incluyen operaciones activas, el monto total de la deuda, el plazo, la tasa de interés efectiva aplicada y su método de cálculo y las comisiones. Se advierte que la tasa de interés pactada y efectivamente pagada por los clientes, en ningún caso podrá exceder el máximo porcentual permitido por la ley y que hoy es de un dos (2%) por ciento mensual.

3. La de mantener informado a su cliente sobre la evolución o el estado en que se encuentre la gestión respectiva.

4. La de poner en conocimiento del cliente los plazos para la formulación de reclamos, de conformidad con la naturaleza del servicio.

5. La de extender los comprobantes correspondientes a las operaciones realizadas, en los cuales debe constar el registro único de contribuyente del banco, la identificación de la operación y su valor.

6. La de entregar una copia del contrato contentivo de la operación realizada, dejando constancia de tal hecho en el contrato original. En todo caso, se considerará nulo el contrato original en el cual consten espacios en blanco que puedan ser llenados de forma unilateral por el banco con condiciones diferentes a las pactadas.

7. La de apegarse a la Ley, los buenos usos mercantiles y a la equidad, en su trato con los consumidores.

Los contratos bancarios de adhesión incluyen, en la mayoría de los casos, cláusulas que favorecen ostensiblemente a las entidades bancarias, aunque autores como Molle (Molle En: Bonfanti, 1980: 24) traten de afirmar lo contrario, sobre la base de casos específicos que a nuestro juicio no se corresponden con la generalidad de la contratación bancaria. Hay que advertir que la Ley 29 establece la nulidad absoluta de las cláusulas abusivas o vejatorias en los contratos de adhesión, en su artículo 62. La Ley considera como abusivas y por lo tanto nulas de nulidad absoluta, las condiciones generales que incluyan ciertas acciones que para los efectos de los bancos pueden ser:

1. La restricción de los derechos de los clientes, aunque tal circunstancia no se desprenda claramente del texto.

2. La limitación o extinción de las obligaciones a cargo del banco. Dentro de esta situación deben considerarse las denominadas cláusulas de limitación o exclusión de responsabilidad, muy comunes en la contratación bancaria.

3. El favorecimiento excesivo o desproporcionado de la posición contractual de los bancos, lo cual determine la renuncia o restricción de los derechos de los clientes.

4. La exoneración o limitación de la responsabilidad de los bancos por incumplimiento o mora.

5. La facultad del banco para, unilateralmente rescindir[1] el contrato, modificar sus condiciones, suspender su ejecución, revocar o limitar los derechos de los clientes, cuando estos nazcan del contrato, salvo en los casos en los que tal rescisión, modificación, suspensión, revocación o limitación, esté condicionada a incumplimiento imputable al cliente.

6. La obligación del cliente de renunciar de forma anticipada a cualquier derecho fundado en el contrato.

7. La renuncia anticipada del cliente de las acciones procesales, términos y notificaciones personales, contemplados en el Código Judicial o en leyes especiales.

8. La existencia de cláusulas ilegibles.

9. La existencia de cláusulas en idioma distinto al español.

El artículo 62 establece la nulidad relativa de las cláusulas abusivas en los contratos de adhesión. Es así que, siempre dentro del marco de la contratación bancaria, podemos señalar que serían relativamente nulas las cláusulas que:

1.Confieran al banco, para la aceptación o rechazo de una propuesta o la ejecución de una prestación, plazos desproporcionados o poco precisos.

---

[1] Para nosotros debería ser resolver el término adecuado, por aludir la Ley a la terminación del contrato por razones de incumplimiento y no en razón de nulidades.

2.Confieran al banco, un plazo de mora desproporcionado o insuficientemente determinado, para la ejecución de la prestación a su cargo.

3.Establezcan indemnizaciones, cláusulas penales o intereses desproporcionados, en relación con los daños por resarcir, a cargo del banco.

La Ley 29 señala en su artículo 64, tratándose de la interpretación de los contratos, que las condiciones particulares de los contratos de adhesión prevalecerán sobre las generales, en caso de que exista incompatibilidad. De esta forma se establece igualmente que las condiciones generales ambiguas u oscuras se interpretarán en favor, en nuestro caso, de los clientes de los bancos.

E. La profesionalidad.

Debe entenderse que para que la actividad o negocio al que nos referimos sea de carácter bancario, es necesario que ésta sea realizada por una entidad bancaria sin la cual no se concibe que pueda denominársele como tal. En este sentido coincidimos con la opinión esgrimida por Garrigues (Garrigues En: Díaz, 1983: 4). Y es que los bancos son los únicos entes que tienen el conocimiento y la capacidad para realizar este tipo de actividad en forma adecuada a las necesidades del público y que en términos generales gozan, en la mayoría de las legislaciones, de facultad legal para hacerlo o como diría Villegas refiriéndose a la actividad bancaria: "es una actividad profesional, realizada por especialistas expertos en esa materia" (Villegas, 1989: 17). Por lo tanto, no resulta difícil concluir que la actividad bancaria es de aquellas que sólo personal exclusivamente dedicado a su tarea y con conocimientos especializados en su rama, o sea profesional, puede realizar como parte de una gran empresa, de allí que la actividad

bancaria sea necesariamente una actividad profesional y que por lo tanto de la misma sólo pueda resultar una responsabilidad igualmente profesional, con todo lo que ello conlleva.

F. El riesgo.

Para algunos (Herrera, 1985: 26), las peculiaridades que presenta la actividad hace necesario que la misma sea sometida a la denominada teoría del riesgo, de esta forma la responsabilidad de los bancos no sería sino una responsabilidad objetiva, en virtud de la cual probándose el daño y la relación de causalidad entre éste y el actuar de los bancos, los mismos serían por ese sólo hecho, responsables frente al cliente. Por ello, el banco debe siempre soportar el riesgo de sus actos, culpables o no, pues es quien saca provecho de sus actos riesgosos. Estamos frente a una clara aplicación de la teoría del riesgo - provecho (Mazeud, 1977: 10), la cual, en materia bancaria, resulta de relevancia, por el número y la autoridad de los escritores que la han defendido (Borja, 1991: 382). Sin embargo la teoría en referencia no esta exenta de críticas, así el mexicano Borja Soriano expresa: "Decir: el hombre debe soportar las consecuencias de sus actos aún ilícitos desde el momento en que causen perjuicio a otro, porque cada uno debe correr el riesgo de su acción, es apartar al hombre de la acción, es condenarlo a la inercia" (Borja, 1991: 382). Quienes propugnan por la teoría del riesgo se circunscriben fundamentalmente a las esferas de la responsabilidad contractual, la responsabilidad por el hecho ajeno y la responsabilidad a causa de las cosas.

G. La integración en un sistema.

Se afirma que "constituyen -los bancos- un conjunto de unidades entrelazadas armónicamente, cuya función general es la prestación monopólica de la actividad intermediadora y creadora del crédito y prestación de servicios conexos" (Villegas, 1989: 17). Los bancos no actúan individual o aisladamente sino dentro del sistema, centro o plaza bancaria a la que pertenecen. Tal criterio resulta confirmado por la propia Ley bancaria, es así que el literal a del artículo cuatro del Decreto de Gabinete 238 de 2 de julio de 1970, establece como objetivo de la Comisión Bancaria Nacional, entre otros, el velar porque se mantenga la solidez y eficacia del sistema bancario. De lo anterior podría igualmente concluirse, que no sería ilusorio pensar que una determinada actuación de un banco podría incidir en un daño para el sistema bancario al cual pertenece o para un grupo de bancos de dicho sistema, los cuales podría pensarse que arguyeran la responsabilidad extracontractual del banco culpable.

H. El servicio público.

El servicio público, cuyo carácter ha sido afirmado principalmente por autores franceses y belgas (Díaz Ramírez, 1983: 22) y adoptado por constituciones como la mexicana y la colombiana. La concepción de servicio público se fundamenta, principalmente, en la idea de que la banca presta un servicio público, es decir satisface una necesidad colectiva. Este elemento es acogido doctrinalmente desde diversos ángulos entre aquellos que, como Miguel Acosta Romero (Ibidem), sostienen que la actividad bancaria por su naturaleza sólo puede ser prestada por el Estado, el cual

carece de la facultad de delegar este servicio público en los particulares y aquellos que sostienen que si bien es un servicio público, el mismo si puede ser delegado por el Estado en los particulares bajo la fórmula de una concesión o en virtud de autorización legal previa, como sucede en Panamá. Este criterio viene defendido por Villegas que manifiesta que "cuando el Estado 'autoriza' a particulares a realizar esta actividad les esta confiriendo un 'privilegio' al permitir el ingreso en una función que está restringida y limitada a quienes reciban esa autorización" (Villegas, 1989: 20). Pero también se deben considerar a los autores que sostienen que el ejercicio de la actividad bancaria si bien tiene una gran trascendencia e importancia para la sociedad, no constituye un servicio público. Y es que el hecho de que se diga que los bancos tienen una función de interés público, no implica el que tal función sea pública. Esta última posición es aupada por Gavalda, Stouflet y Giuseppe Ferri (Díaz Ramírez, 1983: 26).

En nuestra opinión, esta característica de la actividad bancaria afecta al banco en cuanto a su responsabilidad, únicamente en cuanto a que los posibles perjudicados con una acción dañosa del banco podrían multiplicarse por cientos o miles, dado el caso que las inversiones que efectúe el banco con los bienes de capital que se ponen en sus manos, no sea efectuada en forma responsable, de tal manera que ello disminuya o nulifique los derechos de los depositantes o proveedores de dichos bienes de capital ante una posible liquidación del banco.

I. El secreto bancario.

El secreto bancario surgió como una necesidad de ciertos grupos étnicos de proteger su patrimonio de la persecución política, religiosa y racial. El mismo fue reconocido en primera instancia en Suiza, cuando los banqueros de ese país se negaron a revelar información sobre los depósitos de sus clientes, con el fin de no hacer peligrar los mismos. Ello implica que el secreto bancario surgió en primera instancia como una defensa frente a las autoridades y luego fue convirtiéndose en un deber de los banqueros.

El secreto bancario es definido genéricamente como una obligación que tiene fundamento legal. Pero en lo específico citamos a Rodríguez Azuero, quien de forma descriptiva la define de la forma siguiente:

> El secreto bancario, obligación profesional, es en esencia, la necesidad de conservar la privacidad de las fuentes, el destino, la cuantía, etc., de las operaciones celebradas por cuenta de su clientela, así como la de los estados financieros e informes particulares sobre sus actividades comerciales que ordinariamente presentan los clientes a los bancos, como requisito para la tramitación de las distintas operaciones (Rodríguez Azuero, 1990: 120).

Pero el secreto o reserva en el ámbito bancario, resulta ser también, un bien jurídico tutelado. Y tal reconocimiento y protección jurídica tiene como razón de ser, la protección a los clientes de los bancos, que con la finalidad de abrir una cuenta de depósito o de crédito o recibir un préstamo, revelan al banco gran parte de su vida personal, en el entendimiento de que la información relativa a ésta, tanto como la información relativa a sus dineros y otros bienes tangibles estarán debidamente

resguardadas de todo aquel a quien dicho cliente o la ley, no consientan su acceso. Y es que debe tenerse en cuenta el hecho de que los bancos, deslumbrados por los avances de la tecnología, hayan optado por el procesamiento o tratamiento electrónico de la información, implica de forma directa, que los bancos deban redoblar sus esfuerzos para mantener el secreto, confidencialidad o reserva de la información que le transmiten sus clientes, dada la vulnerabilidad de los sistemas informáticos a través de los cuales se produce el mencionado procesamiento o tratamiento electrónico.

El secreto bancario como deber, obliga a todos aquellas personas que por su relación directa o indirecta con el banco tiene acceso a información relativa a las operaciones con los clientes y como defensa, de invoca frente a todo aquel tercero, o sea quien no forma parte de la entidad bancaria o quien no ha sido autorizado por el cliente o por la Ley para tener acceso a la información relativa a los clientes de los bancos.

El secreto bancario protege tanto a los clientes actuales como a los pasados y aun a los clientes potenciales, cuando éstos brindan información al banco para que sea analizada y permita decidir si pueden constituir una relación jurídica con el banco.

Sin embargo, este bien jurídico también tiene limitaciones que sobre todo, tienen a hacer prevalecer el interés público sobre el interés particular. Así constituyen limitaciones al secreto bancario que determinan que el banco deba revelar información sobre las operaciones de sus clientes:

1. Que el solicitante de la información sea una persona que tenga la calidad de parte accesoria de un crédito, como el caso de los fiadores y codeudores.

2.En razón de que el solicitante de la información resulte ser apoderado, mandatario o representante legal del cliente al que hace referencia dicha información.

3.Cuando el banco tiene que revelar la información a las autoridades en razón de procesos judiciales promovidos por el propio banco con la finalidad de hacer valer sus derechos frente a un cliente.

4.Siendo el caso que el banco tenga que revelar información a autoridades públicas o a cualquier otra persona, a solicitud del propio cliente.

5.Cuando el banco tiene que revelar información a los herederos declarados de un cliente difunto.

6.Siendo el caso que quien requiere la información resulta ser una autoridad pública con competencia para solicitar la misma.

La violación del secreto bancario hace incurrir al infractor en responsabilidad tanto civil como penal y administrativa.

En Panamá, la existencia del secreto bancario como institución constitutiva de nuestro ordenamiento jurídico, se ha determinado más que nada por inferencia, ya que no existe ninguna ley que en forma expresa lo mencione. Esto ha implicado que se concluya que el mismo existe con aplicación de criterios doctrinales, analógicos y un argumento *a fortiori,* según la autorizada opinión del Profesor Herrera (Herrera, 1985: 34).

La doctrina extranjera afirma que existe un secreto bancario en países que presentan una legislación similar a la que rige en Panamá. Por ello, con ayuda del método analógico de interpretación, podemos concluir que si en tales legislaciones se concluye la existencia de una secreto bancario, en Panamá el mismo también debe existir.

El argumento *a fortiori,* se esboza en el sentido de que si las normas del Decreto de Gabinete 238, especialmente los artículos 65, 74 y 101, le permiten a los bancos oponer el secreto frente a las autoridades de la Comisión Bancaria, que son

precisamente las instituidas para ejecutar las labores de control y vigilancia del sistema bancario, con mucha más razón deben poder oponerlo frente al resto de las autoridades públicas y por supuesto frente a los particulares no autorizados.

Además de lo anterior, el secreto bancario resulta tutelado en el Código Penal pero como parte del denominado secreto profesional (artículo 170). También el mismo es reconocido de forma expresa en la Ley 18 de 28 de enero de 1959, por la cual se dictan disposiciones en relación con cuentas bancarias cifradas.

CAPÍTULO SEGUNDO: ASPECTOS GENERALES DE LA RESPONSABILIDAD DEL BANCO FRENTE AL HECHO INFORMÁTICO

I. El Hecho Informático Bancario.

A. Concepto.

La informática, término acuñado por Philippe Dreyfus en 1962, ha sido definida como: "la metodología que permite planear y resolver la problemática del trato racional y automático de la información" (Méjan, 1994: 26), también como: "la tecnología para el tratamiento sistemático y racional de la información mediante el procesamiento electrónico de datos" (Ibidem) y más simplemente como "la ciencia que estudia y tiene como objeto el tratamiento automatizado o electrónico de la información" (Jijena Leiva, 1992: 15). A este concepto se asocian algunos otros como el de cibernética, el cual se relaciona más con las redes de control y comunicaciones que gobiernan las computadoras y también se utiliza como sinónimo de la inteligencia artificial que se atribuye a las mismas.

Habiendo precisado el significado de la informática, debemos referirnos a su reflejo fáctico o práctico, o sea a su manifestación en la realidad. Es por ello que anunciamos la existencia de un hecho informático, que al decir de Bustamante Alsina (Bustamante, 1993a: 639), es aquel que incluye a las actividades relacionadas con el tratamiento electrónico de la información. Pero en una definición más amplia, podemos manifestar que el mismo consiste en aquel hecho relativo a ese trato o tratamiento racional, automático y sistemático de la información por medios electrónicos.

En nuestro caso, el tratamiento electrónico al cual nos hemos referido, es el desarrolladó por las entidades bancarias, teniendo por objeto fundamental, la información tanto personal como financiera de sus clientes. Por ello, el hecho informático bancario será aquel que incluya el tratamiento electrónico que realicen los bancos, de la información que les es propia y principalmente de la información que le proporcionan sus clientes.

Este tratamiento electrónico de la información incluye todos los momentos básicos de la actividad informática, a saber: la obtención de datos, su almacenamiento, su procesamiento y la transmisión de éstos. Cabe advertir que por datos, en este caso específico, deben entenderse todos los hechos representados bajo una fórmula convencional apropiada para su comunicación, interpretación o tratamiento que realice el hombre directamente o que se realice por medios automáticos.

Se señala que la gran mayoría de la información bancaria es procesada electrónicamente, por lo que los datos y documentos son transmitidos a través de un banco o entre un banco y sus corresponsales y clientes, mediante conexiones de telecomunicaciones públicas, como pueden ser líneas telefónicas o satélites. Los usuarios de los bancos, ya sean empleados o clientes, acceden a esta información de manera directa mediante terminales de computadoras o teléfonos.

Esta masa de información que recogen los bancos alimenta la memoria electrónica de los computadores, que a la manera de un gigantesco registro, pasan en tal sentido a denominarse bancos de datos. Estos bancos de datos tienen como característica diferenciadora de otros archivos comunes, el hecho de que los mismos resultan "organizados e interrelacionados según atributos comunes, en función de posibles requerimientos" (Delpiazzo, 1990: 385), esto determina la existencia de algunas

cuestiones jurídicas que deben ser analizadas a fondo, entre las cuales destacan: el deber del banco y el derecho del cliente de conocer y solicitar la corrección, cuando fuere el caso, de la información que sobre el mismo se almacena en el banco de datos y el deber del banco y el derecho del cliente de que tal información se mantenga ajena a toda persona no autorizada o legalmente facultada para acceder a la misma.

En el aspecto jurídico, estos hechos informáticos se han manifestado en la existencia de un derecho informático, si entendemos que la informática en general puede ser el objeto de estudio del derecho como ciencia.

Para Delpiazzo, citado por Jijena, el derecho informático se define como: "una parte del orden jurídico, integrada por las normas y principios que regulan el fenómeno informático, y la disciplina cuyo objeto de estudio lo constituye ese sector" (Jijena Leiva, 1992: 22). Otros criterios prefieren expresar una idea más amplia y de carácter descriptivo, pues si bien, el derecho informático incluye normas, reglas y principios jurídicos, su objeto debe fundamentalmente tutelar los derechos de las personas con la finalidad de que estos no sean atomizados por la tecnología, además debe analizar a profundidad la instrumentación de las nuevas relaciones jurídicas que han surgido como resultado de los nuevos bienes informáticos y la transmisión de los datos. Quienes precisan un poco más la materia (Gustavino En: Messina de Estrella Gutiérrez, 1989: 123) que debe ser objeto del mismo, mencionan: la tutela legal de los instrumentos informáticos, la protección de la intimidad, los contratos informáticos, los delitos informáticos, la responsabilidad civil por daños emergentes de la informática y el derecho procesal informático (Messina de Estrella Gutiérrez, 1989: 123). A nosotros nos interesa principalmente, todo lo que tiene que ver con una de estas materias, es decir, la responsabilidad civil por daños emergentes de la informática.

B. Finalidad de la informática bancaria.

La informática contribuye en tres planos al manejo de la información: con una memoria capaz de conservar y restituir datos de forma constante, con la capacidad de combinar automáticamente datos existentes para crear nuevos datos y con la capacidad de operar a una velocidad mayor que los métodos tradicionales. Así las entidades bancarias, necesitadas como el que más, de un sistema efectivo para el manejo de la información, el cual integre los tres planos antes mencionados, recurren a la tecnología informática. Y esta les sirve de medio para agilizar y ordenar sus operaciones, de tal forma que puedan prestar un servicio de mayor calidad y más efectivo a su numerosa clientela o como señala Peña Castrillón (Peña Castrillón, 1979: 10), para conseguir una mayor eficacia de la empresa bancaria, es decir una óptima administración, en momentos en que en gran medida se deja atrás el concepto de banca especializada y se arriba al de banca universal, o sea aquella que tiende a promover la prestación de servicios financieros totales e integrados. Y es que como dice Delpiazzo: "uno de los campos donde la aplicación de la Informática ha encontrado terreno más fértil es precisamente el bancario, donde fue inicialmente incorporada para el ahorro del trabajo, especialmente en tareas contables, y se ha extendido rápidamente a otras áreas, hasta modificar sustancialmente la operativa del sistema financiero a través de la banca automatizada (Delpiazzo, 1990: 369). Haciendo un poco de historia, tenemos que ya

desde la década de los años setenta, se predecía la existencia de agencias o sucursales portátiles, mediante la realización de actividades tales como:

> Terminales financieras localizadas en puntos de venta, operadas tanto por los cajeros como por los clientes.
>
> Compartir terminales cajeras remotas por instituciones financieras.
>
> Sistemas para garantizar y verificar cheques.
>
> Sistemas de autorización de créditos a todo lo ancho del país, los cuales están tanto fuera como dentro de la banca (Peña Castrillón, 1979: 24).

Como podemos comprobar, tales actividades son hoy una realidad cotidiana mediante las denominadas transferencias electrónicas de fondos (conocidas por sus siglas como TEF) que no son más que "aquellas operaciones cuyo fin y efecto es el de transferir riqueza o fondos de un patrimonio a otro sin ningún movimiento efectivo de dinero ni formalidades en el sentido tradicional, sino solamente mediante instrucciones electrónicas impartidas y ejecutadas del mismo modo" (Giannantonio, 1989: 7). Mediante las llamadas TEF los débitos y créditos son efectuados de forma simultánea e inmediata, a través de los sistemas *on line*. Estas transferencias pueden efectuarse o bien por iniciativa del deudor, en los sistemas de transferencias de créditos o del acreedor, en los sistemas de transferencias de débitos. En este sentido se avanza hacia lo que podría denominarse una *cashless society*, una sociedad en la que los bienes circularán por medios electrónicos. Las expresiones tangibles de las TEF las tenemos en: la proliferación de cajeros automáticos o *ATM's* (*Automatic Teller Machines*), los cuales prestan los servicios de caja básicos tales como: depósitos, retiros, informar saldos, pagos de deudas, transferencias de fondos entre cuentas del mismo banco o de otro banco, pagos de tarjetas de crédito, etc.; los puntos de venta o *POS* (*Point of Sales*), que son equipos instalados por un banco o por un grupo de entidades financieras en comercios con

atención de numeroso público y que permiten la compra y venta de bienes y servicios, en ambos casos mediante el uso de tarjetas magnéticas, y la realización de débitos automáticos en las cuentas de sus clientes y acreditación en las cuentas de las firmas vendedoras. Estos últimos pueden también imprimir y entregar talones con la fecha, codificación alfabética de productos adquiridos, forma de pago e imputación a cuentas, con posibilidad de efectuar descuentos automáticos según las políticas de ventas adoptadas (Delpiazzo, 1990: 381); la denominada banca hogareña, que permite al cliente efectuar transferencias de fondos por teléfono desde su domicilio. Este sistema que también puede ser operado a través de computadores personales y televisión por cable, permite realizar consultas, ordenar pagos de servicios a terceros y cancelar créditos; el *clearing bancario automático* o sistema de pago sin papeles (Ibidem), que consisten en el procesamiento de transacciones en cuentas de depósito a la vista, por medios electrónicos, sin la utilización del cheque. Estos sistemas también denominados *Automated Clearing Houses* (*ACH*) son cámaras de compensación automática. Estas tienen por finalidad que los clientes abonen sus cuentas mediante transferencias electrónicas. Se registran las extracciones y los cobros en una cinta magnética u otro medio idóneo, efectuándose los débitos y créditos que correspondan. En los Estados Unidos son relevantes la FEDWIRE, la CHIPS, la CASHMIRE y BANKWIRE, así como también la ya mencionada SWIFT, esta última a escala mundial. Todas estas megaredes prestan este servicio que beneficia a millones de clientes de bancos. También cabe resaltar la denominada conexión automática entre instituciones bancarias, de éstas con el Banco Central respectivo y entre los bancos centrales de diversos países.

Finalmente debemos mencionar, la utilización de la denominada banca virtual, en virtud de la cual los clientes pueden realizar operaciones mediante el uso de

terminales interactivas (con capacidad para dar respuesta a la voz del cliente) y de multimedios (con imagen y sonido).

Los anteriores mecanismos han tenido nuevos avances en los últimos años en vista de la aparición de la denominada tarjeta inteligente, la cual contiene un *chip* o microprocesador con capacidad propia de memoria, de modo que permite no sólo activar un terminal sino memorizar la operación y convertirse en un archivo portátil. La tarjeta inteligente que resulta ser parecida a una tarjeta de crédito o débito, puede ser cargada con dinero E (BusinessWeek, 1995: 48) (dinero electrónico) comprado con dinero tradicional, también puede guardar monedas y dólares digitales cargados mediante líneas telefónicas, desde un banco u otro emisor de dinero E, en un computador personal o una billetera electrónica (dispositivo del tamaño de la palma de la mano utilizado para almacenar y transmitir dinero E). Este dinero digital permite hacer compras en línea, transfiriendo dinero a vendedores de bienes o servicios a través del INTERNET o mediante la televisión interactiva. Últimamente también se menciona la tarjeta láser, que esta dotada de una capacidad de almacenamiento infinitamente superior a la tarjeta inteligente.

A lo anterior hemos de adicionar, la multiplicación de las redes de comunicación y de compensación interbancarias, que no son más que redes de cajeros automáticos tanto nacionales como internacionales (PLUS y CIRRUS) y la existencia del INTERNET. Esta última es una red mundial de computadoras que ofrece servicios de correo electrónico, transferencia de archivos, boletines de noticias, foros de discusión a través de tableros electrónicos y conversación electrónica, inclusive a través de multimedia. Todas estas redes procesan los datos por lotes (*batch*) o en línea.

Las transferencias electrónicas de fondos a través de cajeros automáticos y puntos de ventas, se realizan mediante el uso de una tarjeta magnética. En el plano jurídico, la mencionada tarjeta ha sido objeto de definiciones como aquella que se expresa en el título IX del Acta de Protección al Consumidor de Crédito de los Estados Unidos de América denominada Acta de transferencia electrónica de fondos, la cual define la expresión tarjeta como: "una tarjeta, código u otro medio de acceso a la cuenta del consumidor, con el fin de iniciar una transferencia electrónica de fondos cuando la persona a quien dicha tarjeta u otro medio de acceso haya sido emitido, solicita, recibe, firma, usa o autoriza a otra a usar dicha tarjeta u otro medio de acceso con el fin de transferir dinero entre cuentas u obtener dinero, propiedades, trabajos o servicios".

En cuanto a la utilidad práctica de la tarjeta, debe decirse que sobre una banda de la misma son inscritos magnéticamente algunos datos como el nombre del usuario, el número de la cuenta y la fecha del vencimiento de la cuenta. Con base en tales datos y a un algoritmo[2], la computadora accede al número de identificación del cliente denominado PIN (Número de Identificación Personal por sus siglas en inglés). En estos casos el cliente introduce la tarjeta en la ranura correspondiente del terminal, para que la computadora descifre los datos contenidos en la banda magnética, desarrolle el algoritmo secreto y verifique el PIN. Luego el cliente digita en el terminal su PIN y la computadora coteja tal PIN con el contenido en la tarjeta magnética. Si los dos números de PIN son iguales, se procede con la operación, de otra forma se regresa la tarjeta y no se procede con la operación. De procederse con la operación, el cliente deberá obtener al final de la misma un recibo en el que consten los pormenores de ésta. Tratándose del uso de un punto de venta, el cliente debe exhibir la tarjeta magnética y por medio de la

---

[2] Por algoritmo debe entenderse una fórmula de cálculo.

terminal, ordenar al banco acreditar la cuenta del vendedor, debitando la propia, para lo cual deberá digitar el PIN.

Las anteriores operaciones han permitido la acuñación del concepto de banca electrónica, para denominar a todos los servicios bancarios que se prestan mediante la utilización de sistemas electrónicos de procesamiento de información.

Castro Lechtaler explica el desarrollo de las comunicaciones bancarias al afirmar que: "la integración de los medios computacionales con los medios de telecomunicaciones, pareciera que es la manera más racional, de encarar el problema de mejores y más servicios de comunicaciones, en concordancia con los modernos sistemas informáticos de apoyo a la actividad bancaria" (Castro, 1989: 92).

Por otra parte, la tecnología se ha convertido para los bancos en una herramienta estratégica que le facilita: la mejora en los procedimientos administrativos, contables y de control; el incremento de operaciones y de clientes como resultado de la introducción de sistemas de procesamiento en línea y la consecuente mejora de los servicios al usuario; la mejora en la administración de la tesorería del banco y la automatización de los procesos de canje o compensación; el incremento de la posición competitiva del banco; imagen de adelanto tecnológico ante el cliente y seguridades de la transacción; mejoras en la atención al cliente; aumento en la cobertura geográfica y temporal de atención al cliente; ingresos adicionales por el cobro de comisiones, incrementos en la productividad del personal ante una mejor distribución del quehacer diario; ahorros por la eliminación de las inversiones correspondientes al reemplazo de equipos correspondientes a tecnologías obsoletas; incremento en los controles y seguridad del sistema; ahorros en horas extras; ahorros en microfilmación, utilería y papelería (Serrano, 1989: 103 a 108).

C. La transferencia electrónica de fondos.

En todo caso, las principales operaciones de servicio al público que realizan estos instrumentos de la tecnología, se pueden mencionar bajo la denominación genérica de transferencia electrónica de fondos.

La transferencia electrónica de fondos resulta en la actualidad, la más visible forma en la cual los bancos demuestran como utilizan la informática en la prestación de sus servicios. Esta actividad ha sido descrita como aquella mediante la cual se ejecuta un traspaso de fondos de una cuenta a otra, de tal forma que permite efectuar pagos sin que se produzca un desplazamiento de dinero. Por su parte, el Acta de transferencias electrónicas de fondos de los Estados Unidos define a éstas como:

> Cualquier transferencia de fondos, diferente de una transacción originada por un cheque, letra de cambio, o instrumento similar en soporte papel, que sea iniciada por medio de una terminal electrónica, instrumento telefónico o computadora o cinta magnética de manera tal que ordene, instruya o autorice a una institución financiera a debitar o acreditar en una cuenta. Dicha expresión, aunque sin limitarse a ellas, incluye las transferencias de puntos de venta, transacciones con cajero automático, depósitos directos o extracciones de fondos y transferencias iniciadas por teléfono.

Estamos pues, frente a lo que podríamos llamar un simple juego contable, por el cual se asienta un débito en la cuenta del ordenante y un crédito en la cuenta del beneficiario.

Todas estas operaciones pueden ser realizadas en tiempo real, con disponibilidad casi inmediata para el receptor de la transferencia o en *batch*, o sea

mediante la captura y transmisión de la información dentro de operaciones sistematizadas (Serrano, 1989: 99). La Comisión de las Naciones Unidas para el derecho mercantil internacional (UNCITRAL), resalta el avance tecnológico logrado con este nuevo mecanismo al definir la transferencia electrónica de fondos como: "aquella transferencia de fondos en la que una o más de las operaciones del proceso que antes se desarrollaban sobre la base de técnicas documentales, se efectúa ahora mediante técnicas electrónicas" (Delpiazzo, 1990: 380). Por su parte la Ley norteamericana sobre transferencia electrónica de fondos de 1978, la define como: "toda transferencia de fondos iniciada a través de una terminal electrónica por vía telefónica, computador o cinta magnética de manera de ordenar, instituir o autorizar a una institución financiera para debitar o acreditar una cuenta". Mientras que el concepto terminal electrónica debe indicarnos: "un mecanismo electrónico, distinto de un teléfono operado por un consumidor, por medio del cual el consumidor puede iniciar una transferencia electrónica de fondos. Dicho término incluye transferencias de puntos de venta, cajeros automáticos y máquinas dispensadoras de dinero en efectivo, sin limitarse a ellas" (Ibidem).

Las transferencias electrónicas pueden clasificarse en cuatro formas, según las cuentas que resulten involucradas en las operaciones, así tenemos:

1. Transferencias entre cuentas que un cliente tiene en la misma institución bancaria, ya sea en una sucursal o en distintas sucursales.

2. Transferencias de la cuenta del ordenante a la de otra persona cuando ambas están radicadas en el mismo banco.

3. Transferencias entre cuentas del mismo titular existentes en distintos bancos.

4. Transferencias de la cuenta de una persona abierta en un banco a la de un tercero radicada en otra entidad.

En todo caso, se establece que tal actividad es una operación que puede ser incluida dentro de aquellas que conllevan un servicio de caja que las entidades bancarias prestan a sus clientes y por la cual perciben generalmente una comisión.

Esta actividad tiene, a juicio de Peña Castrillón (Peña Castrillón, 1979: 26), tres consecuencias fundamentales, a saber:

1. La eliminación del uso de papel en la relaciones entre los bancos y entre éstos y sus clientes.

2. La prestación de servicios bancarios fuera del área de las oficinas bancarias.

3. El traslado al banco de una serie de gestiones y el aumento de su responsabilidad, pues al eliminarse el papel, no se elimina el deber de probar las distintas relaciones obligacionales que en el mismo constaban y que constituyen informaciones de las cuales debe darse cuenta de alguna forma y revestirse de la seguridad necesaria.

En la evolución de la transferencia electrónica de fondos cabe resaltar, el cambio de políticas de los bancos, que iniciaron con un almacenamiento descentralizado de la información de los clientes, es decir, por sucursal, y se han movido más hacia la centralización de tal manejo en un solo centro de cómputo o informática, así como la elaboración de mecanismos para el intercambio de órdenes en forma electrónica. Estos último mediante el intercambio físico de dispositivos de memoria o mediante el uso de telecomunicaciones. De esta forma es que aparecieron las cámaras de compensación electrónica y la teletransmisión internacional, mediante la

vinculación a redes de comunicación, y luego la distribución automática de billetes, los cajeros automáticos y las terminales de puntos de venta.

En el caso de las teletransmiciones internacionales, es preciso resaltar el desarrollo de las megaredes electrónicas de comunicaciones interbancarias, generalmente de carácter privado y las cuales procesan órdenes de pago en formatos predeterminados y otros datos diversos. Estas redes fueron creadas con la finalidad de reemplazar los viejos sistemas manuales para el procesamiento de transacciones en el sistema de pagos mundial, facilitando desde su inicio las posibilidades de impartir instrucciones de pagos en horarios más extendidos que el sistema tradicional del telex, abaratando el costo de este tipo de comunicaciones, y aumentando el nivel de seguridad en la etapa de las entregas, toda vez que el banco dueño del sistema de comunicación asumiría la responsabilidad por las instrucciones recibidas, siempre y cuando se transmitieran dentro del horario convenido, así también se redujeron los riegos de alteraciones o fraudes al segregarse las funciones para el procesamiento de operaciones tales como capturas, aprobaciones y la administración del sistema, además el mismo permitió la transmisión encriptada (en clave) (González, 1992: 18). Sin embargo no todo fueron ventajas para estas nuevas redes, pues hubo un aumento en el nivel de riesgos reflejados en errores en la captura de datos, debido a la falta de homogeneidad en los formatos de captura y métodos de proceso de cada sistema privado, en razón de la suscripción de un banco a varios sistemas electrónicos de transmisión de datos. También los costos de automatización sufrieron un aumento debido a la mencionada falta de homogeneidad de los sistemas, además de la falta de movilidad de bancos corresponsales en razón del tiempo de contratación y entrenamiento que determina la implementación de estos sistemas privados de transmisión de datos (González, 1992:

18). Es así como en los años sesenta, 250 bancos de Europa y América del Norte crearon un sistema de comunicaciones conjunto, que fue el precursor de la denominada Societe for Worlwide Interbank Financial Telecommunication S.C. (SWIFT), la cual inició operaciones formalmente el 9 de mayo de 1977. La misma incorporaba para 1990 a más de 3,400 bancos en 83 países. Esta sociedad fue constituida en Bélgica con un carácter cooperativo. Dicha sociedad tiene por principal finalidad el procesamiento de mensajes interbancarios, haciendo posible desde sus inicios: ahorros en el procesamiento electrónico de órdenes de pagos al viabilizar su automatización a nivel interno y la homogeneidad en los formatos de transmisión, pues se dispuso el uso de formatos de carácter universal, lo cual permitió eliminar los problemas de lenguaje e interpretación entre el que envía y recibe mensajes (Franco, 1990: 17), para tales efectos las entidades bancarias miembros de la red se conectaron a la misma a través de terminales basadas en unidades de proceso, denominadas *interfaces*; se automatizó el proceso de codificación y descodificación de mensajes; produjo ahorros en los costos de transmisión; disminución de las alteraciones y los fraudes al incorporar sofisticados sistemas de seguridad, se mantuvo la transcripción encriptada; se codificó mediante el control del conteo de caracteres, se controló la captura de mensajes, la aprobación y administración de sistemas separados y se controló el acceso a la red por usuarios autorizados (*lon-On*) (González, 1992: 19).

Hoy en día, la red SWIFT permite el intercambio de datos a través de 7 categorías que abarcan más de 70 tipos de mensajes, entre los que se pueden mencionar:

1. Transferencias entre clientes.
2. Transferencias interbancarias.
3. Depósitos, préstamos e inversiones.
4. Compra de divisas.
5. Cobranzas.

6. Bonos, acciones y valores.
7. Crédito documentario.
8. Mensajes especiales (Estado de cuenta, conformación de débito o crédito o solicitudes, avisos, cancelaciones y mensajes de formato libre) (Franco, 1990: 17).

En Panamá más de 20 bancos eran miembros de la red SWIFT para 1990.

Actualmente los terminales para la obtención de información bancaria y para efectuar transacciones entre cuentas, también se encuentran en las casas y en las oficinas de los clientes de los bancos, todo ellos a través del denominado *home banking*. Mediante el uso de sus tarjetas de crédito o débito, los clientes pueden consultar saldos y efectuar transferencias entre cuentas a través del uso de terminales electrónicas conectadas con el computador central del banco y suministradas por éstos en venta o *leasing*, e instaladas en las residencias u oficinas de sus clientes. De esta forma, al referirnos a las TEF, no sólo debemos mencionar los cajeros automáticos, sino también los terminales de *home banking*.

D. Otras aplicaciones del procesamiento electrónico de datos y algunos de sus efectos en la actividad bancaria.

Ahora bien, la transferencia electrónica, no obstante ser un hecho informático bancario complejo y transcendente, como hemos visto, no es el único, puesto que el uso de la informática se extiende a todas las operaciones bancarias tales como:

1. Información de clientes
2. Contabilidad General
3. Depósitos Bancarios

4. Emisión de títulos valores
5. Líneas de crédito
6. Préstamos
7. Mercadeo
8. Tesorería
9. Informes
10. Auditorías
11. Recursos Humanos
12. Correo Electrónico
13. Sistema de información gerencial
14. Procesadores de Palabras

Actualmente existen aplicaciones especiales para ciertas áreas del banco tales como manejo de cajas y plataforma.

Esta evolución de la actividad bancaria determina que el ordenamiento de la información que deben realizar los bancos, no sea de carácter común, sino que muy bien pueda calificarse como científico o profesional.

Ahora bien, el uso de los mencionados sistemas informáticos en la actividad bancaria, conlleva la existencia de variados riesgos, es decir, situaciones en las cuales la naturaleza del procesamiento electrónico de la información puede implicar daños a los clientes de los bancos o terceros o aún al propio banco, cuando esto sucede, estamos ya no frente a un simple hecho informático, sino más bien frente a un hecho ilícito informático. Lógicamente a nosotros nos interesan aquellos en los cuales el banco es susceptible de asumir alguna responsabilidad para con sus clientes o terceros ajenos a éste. Un ejemplo de tales riesgos, lo observamos muy a menudo cuando los sistemas

informáticos están fuera de operación, pues en tales casos, los efectos perjudiciales en el tiempo real de los servicios bancarios a los clientes son inmediatos y se incrementan rápidamente. La acumulación de material pendiente para procesar se desarrolla rápidamente y, después de un daño que dure varias horas, dicho material tarda días en despacharse. Especialmente desbastadores son los efectos en el caso de las transferencias electrónicas de fondos y de los sistemas de pago, en particular, aquellos que garantizan un servicio de liquidación en el mismo día, cuyos beneficiarios dependen del recibo de fondos para cubrir sus compromisos. Los costos derivados de una falla grave en los sistemas pueden superar los de reposición de los equipos, datos o *software* dañados (Superintendencia Bancaria de Colombia, 1990).

Cuando un banco queda imposibilitado a pagar debido a problemas en el sistema, los bancos que tienen préstamos pendientes con dicho banco incurren así mismo en incumplimientos y éstos pasan a lo largo del sistema en una reacción en cadena que puede abarcar y paralizar todo el sistema de pagos. En algunos casos, cuando estas cosas ocurrían, el remedio clásico era volver a realizar manualmente los procesos que el sistema había invalidado. Sin embargo, hoy en día este procedimiento no resulta posible en muchos casos, pues son pocos los bancos que podrían funcionar sin sistemas de informática.

Los riesgos también tienden a aumentar como señala Borda: "si se considera que se puede acceder a los ordenadores intangiblemente, sin dejar rastros del uso del sistema y de manera instantánea" (Borda, 1990: 330). Inclusive se señala sobre este particular,

que aunque el *software* tenga protección, existen los denominados violadores de protección de programas o *crackers*, los cuales inutilizan cualquier defensa.

Borda (Ibidem) enuncia también una clasificación de estos riesgos atendiendo a su relación con la operación o actividad de los bancos, incluyendo en esta los aspectos:

1. Financieros: relacionados con la exactitud y confiabilidad de los registros contables y financieros, protección de activos y el cumplimiento requerido de políticas, procedimientos, leyes y regulaciones.

2. Operacionales: relacionados con la eficiencia, productividad y rentabilidad de las operaciones.

3. Administrativos: relacionados con información gerencial exacta y adecuada, cumplimiento global de objetivos, estrategias y planes.

Así también se señala la existencia de riesgos derivados de la automatización y se incluyen los relacionados con:

1. Los medios: daño del computador, daño de las cintas, discos, disquetes, daños en la transmisión, etc.

2. Errores: de transmisión, de programación, de operación, etc.

3. Intencionales: violación de la privacidad, fraudes usando el computador, etc.

Aquellos de estos riesgos cuya ocurrencia conlleva un daño al cliente o terceros, serán tratados más a fondo en el capítulo siguiente.

E. La informática bancaria en Panamá.

En Panamá la informática bancaria se ha desarrollado a partir de finales de los años sesenta según Eudoro Jaén (Jaén, 1996: 21 a 26), quien señala que para finales de la mencionada década, los bancos de la localidad inician la instalación de "computadoras", o más bien máquinas electromagnéticas que utilizan el principio de tarjetas con bandas magnéticas, en reemplazo de las tarjetas perforadas utilizadas hasta ese momento.

En la década de los años setenta, se activa la comercialización de los equipos de cómputo. Los primeros bancos en desarrollar programas de innovación tecnológica son: el Banco Nacional de Panamá, The Chase Manhattan Bank, N.A., Citibank, N.A. y el Banco Exterior de España. No obstante los sistemas instalados están orientados a realizar cálculos periódicos (cálculo de intereses) y procesos en *batch*es (por lotes de datos). Realmente se trata de procesamiento de datos tradicionales con el fin de descontinuar los procesos manuales realizados principalmente para operaciones de préstamos, cuentas de ahorros, cuentas corrientes, contabilidad, planillas y otros.

Finalmente, aparece la minicomputadora como alternativa a las computadoras grandes, también denominadas *mainframes* y las microcomputadoras, las cuales son utilizadas principalmente como procesadores de palabras y que luego se utilizan para labores más sofisticadas como el desarrollo de aplicaciones y las bases de datos.

Para la década de los años ochenta, se produce en forma acelerada la total automatización de las operaciones bancarias en el sistema bancario panameño.

En 1985, la Caja de Ahorros inicia el desarrollo de su plan tecnológico, el cual consigue la total automatización de sus operaciones.

El resto de los bancos de la plaza panameña introducen el concepto de sistema distribuido, con un *mainframe* soportado por equipo de rango intermedio por regiones, cuyo objetivo era la creación de archivos regionales y la toma de decisiones a nivel regional. Es el Banco Nacional de Panamá quien inicia este desarrollo a través de sus centros regionales en Chitré, David y Colón.

A fines de la década, según Jaén, se consolida el concepto de plataforma de servicios automatizada, o sea el área de servicios al público, permitiendo que la toma de decisiones se baje al nivel de la apertura de la cuenta; también se desarrolla la denominada banca electrónica, el teleproceso y los productos de *cash management* o manejo de liquidez para beneficio de los clientes corporativos, lo cual permite la comunicación directa entre el cliente y el banco y consecuentemente el envío y recepción de instrucciones.

En los años noventa, se intensifica el uso del teleproceso para realizar transacciones monetarias. Se persigue bajar los niveles de afluencia de público a las sucursales. Más tarde empiezan a utilizarse los cajeros automáticos y los sistemas de audio-respuestas. El sistema de arquitectura abierta permite a los bancos alejarse de los *mainframes* e introducir el sistema de cliente-servidor, sobre la base de computadores personales con terminales inteligentes que permiten adoptar decisiones en la propia estación de trabajo.

Los bancos empiezan a utilizar la tecnología informática para otros fines distintos del simple procesamiento de información, tales como el mercadeo de sus productos y para mantener adecuadamente informados a los niveles gerenciales a través

de los sistemas de información gerencial. Ya no se manejan sólo productos sino clientes, en función de su relación con el banco, esto permite la promoción y venta directa de servicios y productos. La automatización de la plataforma o área de prestación de servicios directos al público, facilita la casi inmediata referencia de saldos, aprobación de ciertas transacciones, comprobación de firmas y otras actividades similares.

Durante esta década se populariza el uso de los cajeros automáticos, sobre todo a partir del establecimiento de las redes de cajeros y la introducción de los llamados puntos de venta.

En la parte operativa, se inicia el uso de lectores de caracteres magnéticos, lo cual permite el procesamiento de cheques a alta velocidad. Igualmente se introduce la tecnología de imágenes para archivos históricos, esto resuelve los problemas de archivos de grandes cantidades de papel.

La Asociación Bancaria de Panamá ha elaborado un borrador de anteproyecto de ley sobre el almacenamiento tecnológico de documentos, el cual tiende más que nada a tratar de regular el discutido tema de la autenticidad del documento electrónico. Sin embargo, tal como se infiere de los señalamientos del abogado Octavio del Moral (Del Moral, 1996c: 25), esta reglamentación aún debe ser mejorada para conseguir el objetivo de modernización del Centro Financiero Internacional, con la seguridad jurídica que el mismo reclama.

II. Naturaleza jurídica de la responsabilidad de los bancos frente al hecho informático bancario.

El tratamiento de la información por parte de los bancos, determina que éstos asuman responsabilidades tanto en el momento en el cual reciben dicha información, como cuando la procesan y en el curso de sus diferentes aplicaciones. Esto por cuanto que al utilizar los bancos la informática como instrumento operativo, pueden causar daños a sus clientes, es decir, lesionar un bien o interés jurídico perteneciente a tales clientes. Por lo tanto, resulta relevante analizar dicha responsabilidad tanto en lo que corresponde a los daños que causen a sus clientes y aun a terceros en razón de los hechos informáticos que su actividad provoca.

Sobre este particular, hay que tomar en cuenta que el principio de que no hay responsabilidad sin culpa se encuentra en decadencia y viene siendo superado por una responsabilidad objetiva, cada vez más afianzada. Con ello se dice que hoy el centro de atención del derecho de daños se fundamenta en el daño y no en la culpa, como factor de atribución de la responsabilidad. Sin embargo, dicho daño requiere un criterio legal de imputación, criterio este que en muchos países, como el caso de Panamá, no se tiene. Aferrándose éstos todavía, al viejo concepto de responsabilidad subjetiva fundamentada en la culpa.

A. Responsabilidad Contractual.

La relación entre el banco y sus clientes tiene por antecedente necesario un contrato que constituye el instrumento regulador de la relación entre ambas partes. Así resulta lógico concluir que los efectos jurídicos adversos que de los hechos informáticos pueden resultar para los clientes de los bancos, en función de esa relación banco-cliente, deben ser regidos igualmente por los contratos que estos han celebrado y por lo tanto la responsabilidad que surgirá para el banco, en estos casos, debe ser contractual. Un ejemplo clásico de este tipo de responsabilidad ocurre cuando tratándose del contrato de cuenta corriente bancaria, un banco paga un cheque sin fondos, creyéndose que existe dinero en razón de una información errónea del computador. También puede acontecer que el cheque se pague en razón de fondos existentes en otra cuenta corriente, la cual no tiene ninguna relación con el cuentacorrentista que expidió el cheque y todo nuevamente por un error de programación o por un mal uso del computador. En este último caso, puede inclusive dejarse al descubierto la cuenta afectada, con la consiguiente producción de intereses y el rechazo de cheques posteriores por falta de fondos. Todo lo cual conllevará que el cliente sufra un daño, el cual debería ser reparado por el banco.

En materia contractual y principalmente en materia bancaria, actividad que como hemos concluido es de carácter profesional, debemos establecer si las obligaciones del banco relacionadas con el uso de la informática en la prestación de sus servicios, generan obligaciones de medios u obligaciones de resultado?

La anterior interrogante resulta absuelta entre otros por Vázquez Ferreira (Vázquez En: Parellada, 1990: 291), quien nos dice, haciéndose eco de las modernas tendencias en materia de responsabilidad civil, que en materia de las prestaciones que resultan de los contratos relacionados con servicios informáticos, existe una obligación de seguridad en cuanto a la certeza, competitividad y oportunidad del servicio o información al cual se obliga el prestatario. Siendo esta entonces, una obligación de resultado, que sólo exime de responsabilidad si se prueba la culpa de un tercero por quien no se debe responder o por un caso fortuito extraño al riesgo del sistema. En este caso, aunque el banco sólo utiliza el *hardware* o *software* para la prestación de sus servicios, las deficiencias de tales herramientas tecnológicas que provoquen daños a sus clientes, serán por cuenta del banco, quien deberá asumir en principio, la responsabilidad por tales hechos.

En otro sentido, afirmamos que la responsabilidad del banco para con su cliente en materia informática es profesional, puesto que si bien el banquero no es necesariamente un profesional de la informática en sentido general, si lo debe ser de la informática bancaria, es decir de lo que atañe al procesamiento electrónico de la información bancaria, pues para ello asume las consecuencias positivas y negativas de procesar electrónicamente la información de su clientela. Por tal razón, las obligaciones de los bancos serán en términos generales obligaciones de resultado. Ello es así por que éstos últimos tienen que brindar una información correcta y rápida a sus clientes sobre sus negocios con el banco, sin que terceros no autorizados tengan acceso a la misma, lo cual debe cumplirse sin que se admitan excusas sobre su actuar o pruebas de la inimputabilidad de su incumplimiento o cumplimiento defectuoso como señala Messina (Messina, 1989: 130). De su carácter profesional, también deriva la aplicación de la

regla *probatoria probatio incumbit facilius probandi*, o sea que aquel que se encuentra en mejores condiciones para demostrar el origen de un daño, es quien debe ser gravado con la carga de la prueba. Resulta más que lógico suponer que siendo el cliente casi siempre un lego en materia informática, le sería bastante difícil demostrar la existencia de un hecho informático del cual se derive un perjuicio para sí mismo, por ello el referido principio tiene por finalidad que, invirtiendo la carga de la prueba cuando ello sea necesario, sea el banco el que tenga que demostrar la existencia o inexistencia de hechos informáticos de los cuales se derive una consecuencia jurídica negativa, o sea, un daño en contra alguno de sus clientes.

Las obligaciones de los bancos anteriormente mencionadas, se derivan no sólo de las cláusulas contractuales en sí, sino también de las disposiciones legales que forman parte de éstos en razón de lo que dispone el artículo 30 del Código Civil. Sin embargo, la notoria falta de disposiciones legales en relación con esta especializada área del derecho, ocasiona la proliferación de extensos contratos en los que se advierte la inclusión por los bancos de cláusulas exoneratorias de responsabilidad frente a sus clientes, muchas veces criticadas y de dudosa valides (Delpiazzo, 1990: 384).

Las cláusulas de exoneración, liberación o limitación de responsabilidad, no han sido reconocidas tratándose de dolo o culpa grave, o como señalan los norteamericanos tratándose de obligaciones esenciales o fundamental *breach*, ello es así por cuanto que la libertad contractual no resulta aplicable cuando a través de la misma se trata de escapar a la observancia del deber de no dañar a otro, además de que se dice que la ley civil debe proteger al hombre contra su propia imprudencia y sobre todo contra la sorpresa de su consentimiento. Inclusive, no faltan quienes argumentan que la aceptación de una libertad contractual absoluta, como la que fundamentaría el

reconocimiento de este tipo de cláusulas, implicaría un atentado contra el orden público económico.

Bien lo dice la Dra. Glen de Tobón cuando afirma que: "La primera reacción de un banco cuando pone en movimiento un servicio nuevo para muchas personas, es trasladarles enteramente su responsabilidad. Léase si no cualquier fórmula de contrato de cuenta corriente, o de cualquier otra operación masiva, donde los abogados se solazan en incluir cláusulas eximentes de responsabilidad para el banco" (Glen, 1983: 137). Esto es así porque los bancos pretenden declarar que cualquier error cometido o cualquier fraude que atente contra la transferencia de los fondos o de cualesquiera otra operación, será por cuenta del cliente, lo cual coloca al cliente en una posición de inferioridad jurídica, pues el mismo será la mayor de las veces un ignorante del denominado *modus operandi* de la informática y aún menos de sus derechos y obligaciones, además de que al incurrirse en un acto perjudicial para sus intereses, tendrá gran dificultad para probar el origen del mismo y por lo tanto adjudicar la responsabilidad correspondiente.

Recordemos que las cláusulas sobre limitación o exoneración de responsabilidad a favor de los bancos como proveedores de servicios informáticos, e inclusive aquellas que determinan la renuncia de derechos por parte de los clientes, son consideradas absolutamente nulas en los términos del artículo 62 de la Ley 29 de 1 de febrero de 1996 (Supra, págs. 51).

Por razón de lo anterior, la jurisprudencia extranjera y la doctrina, han venido generalmente en defensa de la parte más débil y propugnan en materia bancaria por el imperio de la responsabilidad objetiva y de la responsabilidad por el riesgo creado, en virtud de la cual la responsabilidad debe recaer independientemente de los que diga el

clausulado del contrato o de la prueba de la culpa, en la empresa que busca y obtiene un provecho económico creando dicho riesgo -teoría del riesgo provecho- (Mazeud, 1977: 10) y no en el cliente. Aquí no cabe entonces ampararse en cláusulas de exoneración, liberación o limitación de responsabilidad, pues frente a una responsabilidad objetiva las mismas se tienen por no puestas.

En los Estados Unidos de América, las cláusulas de limitación de responsabilidad han sido tratadas a través del denominado *tort of misrepresentation*, con base en el cual se han formulado demandas de daños, cuyo resarcimiento ha sido reconocido tomando en cuenta la existencia de falsas representaciones de los convenido y circunstancias objetivas que justificaron la confianza en el proponente de un servicio.

Ahora bien, para los efectos de aceptar la aplicación de la teoría del riesgo, debemos establecer si la informática es una cosa o actividad peligrosa. Se argumenta también (Bergel, 1989: 167), que la multiplicidad de campos a los cuales se aplica la informática, así como la necesaria automaticidad de los procesos en que interviene y su natural aptitud para generar daños de toda índole (sean estos contractuales o extracontractuales) determinan que la misma sea potencialmente peligrosa. Otros autores (Bergel, 1989: 167) señalan que ya constituye un principio pacífico, el hecho de que actividades peligrosas no sólo son las previstas en las leyes de seguridad pública o en leyes especiales, y agregan que existen actividades que si bien en principio no presentan como característica típica la peligrosidad, pueden volverse peligrosas si se les desarrolla de cierta forma y no lo son si se les desarrolla de forma distinta, lo cual resulta aplicable a las actividades conectadas con la realización de programas, las cuales no son peligrosas en inicio pero pueden serlo en función de la operación con que se relacionan. Así se dice que la producción de *software* para el desarrollo de actividades

que pueden generar peligro, deben considerase actividades peligrosas. Por ejemplo: el tráfico aéreo, el tráfico terrestre, las instalaciones eléctricas o nucleares, los procesos industriales, etc. Sin embargo, esto en materia bancaria sería discutible, pues en este caso habría que concluir que la actividad bancaria es en si peligrosa, para poder determinar que la producción de *software* con aplicaciones bancarias es una actividad también peligrosa.

No obstante lo anterior, resulta honesto advertir que algunos analistas del tema aun son renuentes a aceptar esta teoría, sin embargo la mayoría considera que al menos la denominada gestión de banco de datos es una actividad peligrosa, no así en lo que se refiere al *hardware* o el *software*, temas sobre los cuales la discusión es mayor.

En lo que se refiere específicamente a la responsabilidad contractual que resulta para el banco como gestor de un banco de datos, debemos establecer que el banco se obliga ante todo a suministrar información correcta, lo cual también implica suministrar información actualizada. De la corrección y actualización de la información dependerá el que no se afecten bienes jurídicos tales como el patrimonio, la intimidad, el honor y la identidad del cliente; además, esta información debe suministrarse en tiempo útil y en forma periódica. Aunque resulta pertinente advertir que en este último caso podría el banco alegar su irresponsabilidad, si las operaciones del sistema informático resultan interrumpidas por causas de fuerza mayor como los constantes defectos en el sistema de telecomunicaciones.

Es claro que las mencionadas obligaciones tienen una relación de especie a género con la de rendir cuentas, por lo que a las anteriores deberemos añadir la obligación de reserva o confidencialidad.

Cabe concluir que si la responsabilidad del banco se tiene por contractual objetiva, estas obligaciones serían de seguridad y por ende de resultado.

B. Responsabilidad Extracontractual.

Por otra parte, los bancos en el ejercicio de la actividad que les es propia, no sólo se relacionan con sus clientes sino que también interactuan algunas veces con terceros, aunque en tales situaciones, prescindiendo de un instrumento contractual que previamente regule dichas relaciones. Dentro de este interactuar, los terceros también recurren en algunos casos a los bancos para solicitar información, y siendo el caso que por disposición legal o por contar con la autorización de sus clientes, tales terceros pueden tener acceso a los bancos de datos de las entidades bancarias, es decir a la información que sobre sus clientes éstos procesan electrónicamente, también tienen la ocasión de beneficiarse o perjudicarse con la corrección o incorrección de dicha información. Es así que no habiendo relación jurídica previa entre el banco y tales personas, la responsabilidad ha de resultar extracontractual. Pero también será extracontractual la responsabilidad del banco cuando la misma sea derivada del delito.

Mucho se ha escrito recientemente sobre la existencia del denominado delito informático, o sea el delito instrumentado mediante el uso de computadoras. Lo cierto es que en nuestro país, cuya Legislación reconoce que de todo delito surge una responsabilidad civil (art. 119 del Código Penal), aun carece de los tipos penales que permitan con certeza afirmar que en nuestro país se castiga, lo que en otros se conoce como el delito informático. Y es que se habla de una concepción materialista tradicional

en los códigos penales, que no admiten un delito sin la existencia de una cosa (el cuerpo del delito) para la configuración de ciertos delitos. No existe como conducta tipificada en nuestra Legislación, ni la intromisión en la memoria de un computador con el fin de debitar fraudulentamente la cuenta de un cliente para proveerse de fondos ajenos, ni tampoco aquella que consiste en un acceso ilícito para destruir o distorsionar la información almacenada en la memoria de dicho computador. En lo que a los tipos tradicionales se refiere, no podemos decir que un computador puede ser objeto de engaño (inexistencia de un sujeto pasivo); para aquellos que piensan que en el tipo estafa puede incluirse estos delitos; ni resulta posible pensar, que la sustracción de un bien inmaterial o incorporal como la información, que además se encuentra contenida en un soporte físico distinto a la misma, puede ser objeto de tipificación bajo el concepto de hurto o robo; que se tipifiquen algunas de estas conductas como falsificación cuando aun se plantea la duda sobre la consideración de los datos y programas como documentos en lo que atañe a la responsabilidad penal; tampoco puede pensarse en la existencia de un daño tratándose de bienes intangibles, como cuando uno o un grupo de datos resulta dolosamente destruido. Lo cierto es que por la aplicación del principio de legalidad de la ley penal (art. 1 del Código Penal y art. 31 de la Constitución Política), que excluye cualquier recurso a la analogía como fuente de derecho, tales supuestos no constituyen ilícitos penales o delitos. También en virtud de lo antedicho, no estamos de acuerdo con aquellos que como Guerrero Mateus y Santos Mera proponen como fórmula de solución: "ampliar ciertos tipos penales para alcanzar a cobijar las conductas delictivas informáticas, bajo denominaciones que con bastante anterioridad ya se habían establecido para considerar delitos comunes" (Guerrero y Santos, 1.993: 33). Sí coincidimos con autores como Jijena Leiva, que al comentar en sentido general la panorámica del derecho comparado afirma: "la aplicación de los

sistemas de información a fines ilícitos no se encuentra tipificada en los Códigos Penales..... , lo que hace imperiosa su incorporación, sobre todo..... en los casos en que los hechos delictivos sólo pueden cometerse mediante el empleo de un sistema informático" (Jijena Leiva, 1992: 71). Cabe señalar que para el jurista Uhlrich Sieber (Sieber En: Jijena Leiva, 1992: 78) la responsabilidad penal debería ser considerada como la *ultima ratio* en materia informática, proponiendo además, la total exclusión de las conductas culposas. Este criterio, del cual se infiere la falta de penalización de la responsabilidad dimanante de los hechos ilícitos informáticos en ciertas áreas, resulta plasmado en recientes producciones jurídicas como el Proyecto Chileno de Legislación Informática, el cual incluye dentro de un ámbito exclusivamente civil, la responsabilidad dimanante del ilícito informático cuando éste afecta el bien jurídico intimidad, es decir se tutela civilmente todo lo relativo a la información personal también denominada nominativa y se incluyen como delitos informáticos a supuestos tales como: "el acceso indebido, el apoderamiento, la destrucción, inutilización, transformación o desfiguración de una información con el fin de impedir u obstaculizar su procesamiento automático o de revelarla o transmitirla indebidamente" (Bergel, 1989: 24 a 25).

Sin embargo, últimamente se ha difundido la tesis de considerar la información registrada como bien jurídico susceptible de tutela, tanto en el ámbito civil como penal, sobre todo basado en hechos tales como: que la información es un bien económico, que es susceptible de adquisición y de creación, y que es equiparable a la reputación u otros bienes inmateriales tutelados. Sobre esto Guerrero Mateus y Santos Mera (Guerrero y Santos, 1993: 54) nos dicen que cuando cualquier persona sustrae dolosamente el registro de un dato y lo graba en un soporte propio con la finalidad de apropiárselo, está

cometiendo un hurto (en la transferencia del dato lo sustrae cancelando en uno un soporte y reproduciéndolo en otro); pero si el registro es borrado o eliminado con el único propósito de perjudicar, pues no se hace ninguna transferencia del dato a otro soporte, responderá por el daño no en el computador ni tampoco sobre las cintas o discos, sino como un daño en el registro como un bien autónomo. Si esta tesis, que considera la información como bien jurídico autónomo logra prosperar, habría mayor oportunidad de considerar los denominados *computer crimes* o delitos informáticos sobre la base de los tipos delictivos tradicionales (Ejemplo: el hurto, apropiación indebida o daños).

El denominado *computer crime* es definido por la Organización para la Cooperación Económica y el Desarrollo como "cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos". Pues bien, a nuestro juicio, nuestra Legislación no penaliza de forma clara estas conductas, por lo cual afirmamos que la víctima de las mismas, hoy en día, sólo puede irrogar con certeza, la responsabilidad civil extracontractual al ofensor, con fundamento en el artículo 1644 del Código Civil, para de tal forma buscar la reparación de su derecho lesionado.

En otro aspecto, cabe advertir que en el caso de la responsabilidad extracontractual del banco, ésta podría ser la que corresponda a su calidad de dueño, guardián o principal del equipo de cómputo, incluyendo *hardware* y *software*. Así opinan quienes señalan que tratándose de la responsabilidad del proveedor de los servicios informáticos y de los empleados del usuario del mismo -en este caso el banco- puedan responder el proveedor del equipo, del programa o de los datos, como así también el operador-dependiente del usuario que lo harán en forma concurrente,

pudiendo el principal ejercer la correspondiente acción de reintegro contra ellos (Borda, 1990: 333). Sobre este particular hay también quienes propugnan por que se considere como un hecho cierto que la responsabilidad del empleador -en este caso el banco- por las acciones de sus empleados, es limitada, sobre todo tratándose de actos ilícitos.

La posibilidad de los empleados del banco de causar daños a sus clientes, en estos casos, resulta alta, fundamentalmente por su capacidad de acceder al sistema informático mediante el conocimiento de claves de acceso y la disposición de los mecanismos de firma automática o electrónica.

Los empleados del banco tienen plena capacidad para manipular tanto el *input* (entrada de datos) como el *output* (salida de datos) del banco, en tal sentido un empleado puede perfectamente programar la computadora para acreditar su cuenta y borrar todo el rastro de la transacción, puede crear cuentas ficticias, etc. Sin embargo conforme a sus deberes técnicos, según veremos más adelante (Infra, pág. 111), el banco tiene el deber de programar la computadora de tal manera que la misma deje la pista de verificación completa de la operación, incluida la orden de borrar transacciones. Así se recomienda, que las personas que programen tal pista, sean distintas de las que preparen los programas de aplicación y desde luego revisen los programas antes de que entren a operar por medio de una auditoría independiente.

Por otra parte, son distinguibles tanto la responsabilidad que surge de un fraude a través del acceso a registros de cuentas o al equipo como parte de la relación laboral, siendo en tal caso responsable el empleador, como la responsabilidad por pérdidas ocasionadas de un fraude que sea posible gracias a los conocimientos que el empleado haya adquirido en el curso de su trabajo y sobre lo cual el empleador no tendría responsabilidad.

En el derecho estadounidense, lo difícil del resarcimiento dimanante de las acciones legales comunes, han inducido a buscar soluciones en los denominados *torts theories*. Así se habla del *tort of Negligence*, el cual se fundamenta en la violación del genérico deber de negligencia, es decir que cuando se realiza una determinada actividad se debe actuar con la cautela exigible a una persona razonable y con conocimiento de los peligros que puede tal actividad producir a terceros. Por ello, se señala que el deber de ejercer *rasonable care* no resulta una circunstancia eximente por haber sido la actividad realizada a través de una computadora. En este sentido, al ser imposible obtener o garantizar una absoluta corrección o infalibilidad del programa, la negligencia implicará la obligación de resarcimiento cuando haya un descuido por parte del elaborador del mismo, como cuando se prescinde de las operaciones de prueba.

También se introdujo el *tort of computer malapractice*, el cual sin embargo tuvo la dificultad que conlleva la individualización del sujeto responsable, en vista de la complejidad de la materia. Por ello la Corte Suprema de los Estados Unidos se ha opuesto a la creación de este *tort*. Sin embargo, el mismo podría ser aceptado en la medida en la que se reconozca la existencia de peritos en materia informática.

La dificultad que implicaban estos criterios de imputabilidad subjetiva determinó que la doctrina se inclinara por criterios de carácter objetivo, con lo cual se reemplaza el factor negligencia por el factor daño.

C. Naturaleza de la responsabilidad tratándose de la gestión de bancos de datos.

Demos un tratamiento especial al análisis de la gestión que hacen las entidades bancarias de los denominados bancos de datos, siendo esta una de las principales, sino la principal actividad de los bancos en su relación con sus clientes.

En este aspecto, tratándose de la responsabilidad por daños, se acentúa más la función preventiva. En los países que como Panamá, carecen de leyes de datos (Infra, págs. 151 y siguientes), la norma genérica de responsabilidad extracontractual (artículo 1644 del Código Civil) de carácter subjetivo, es la única aplicable. En los países con más desarrollo en materia informática, las leyes de datos de carácter objetivo, cumplen esta función. No obstante, se señala que el criterio subjetivo cumpliría una función más adecuada con la función preventiva, en cuanto a los daños evitables o típicos, mientras que el criterio objetivo lo sería para los daños inevitables e imprevisibles.

En materia de responsabilidad contractual, en relación con la gestión de bancos de datos, la doctrina (Bergel, 1989: 209) se inclina por el criterio objetivo, sobre la base de las obligaciones de garantía que se derivan de dicha actividad. En este sentido, se indica que la actividad en referencia debe considerarse como peligrosa sobre todo cuando la misma involucra la recolección o almacenamiento de información sensible (Infra, págs. 145 a 146) relacionada con la intimidad de las personas. También se argumenta que la información procesada electrónicamente, como una forma de energía electromagnética apropiable y valorable, debe sujetarse al régimen legal de las cosas y en tal razón debe quedar incluida en los supuestos de la antedicha responsabilidad objetiva sobre la base de que siempre es susceptible de crear un peligro potencial.

La consideración como responsabilidad objetiva por cosa o actividad peligrosa de la actividad informática, resulta indiscutiblemente aceptada cuando un programa se destina a actividades que puedan importar peligro para el usuario y terceros, en forma difusa.

No obstante lo anterior, como contrapunto, hay quienes se inclinan por la clásica responsabilidad subjetiva fundamentada en el dolo o la culpa del operador o controlador del sistema informático, como es el caso de Bustamante Alsina (Bustamante Alsina, 1993a: 641). Este criterio resulta importante por cuanto que si bien no es el mayoritario en la doctrina y en el más desarrollado derecho comparado, sí es el que sigue nuestra legislación, la cual carece por completo de normas específicas en la materia que nos ocupa. En este sentido, se expresa que la mencionada responsabilidad sería directa por el hecho del hombre sobre aquellas cosas que le sirven de instrumento (Bergel, 1989: 209). Y es que se dice que si bien los sistemas informáticos se desarrollan a través de máquinas, o sea las computadoras, incluyendo la unidad central de procesamiento (*CPU*, por sus siglas en inglés) y sus componentes periféricos, el procesamiento y tratamiento de la información por medios interconectados, así como la elaboración de los programas son el resultado de la acción del hombre. Esto hace que infiramos que para que se invoque la responsabilidad subjetiva debe haber una activa participación del operador de la computadora, pues en caso contrario, si es la cosa la que interviene activamente en la producción del daño, la doctrina sostiene la necesidad de invocar una responsabilidad de carácter objetiva.

Pero a las dos posiciones anteriores, se añaden los siempre presentes eclécticos, quienes promueven el criterio de que la responsabilidad puede ser objetiva o subjetiva,

dependiendo de si la misma proviene de dolo o culpa del operador de la computadora o del vicio o riesgo (Bergel, 1989: 210).

Hay quienes proponen que debe destacarse la responsabilidad objetiva, tomando como factor exclusivo de atribución el riesgo. Y es que a juicio de los que esto señalan, la gestión de un banco de datos es de por sí una actividad riesgosa, toda vez que la información almacenada es siempre susceptible de producir daños si la misma se difunde fuera de los límites previstos originalmente.

El carácter contractual de la obligación se traduce, en el hecho de que el gestor del banco de datos siempre tiene un deber genérico de cuidado sobre la información. Deber de cuidado que se aumenta por factores como: el gran volumen de información que puede ser almacenado, la rapidez con que dicha información puede ser examinada y lo reducido del personal que opera el banco de datos, hecho este último que facilita la labor de terceros interesados en tener acceso a la información. Todo ello implica que de no aceptarse el criterio objetivo, la víctima de una violación de la intimidad, vería frustrada la reparación de su derecho lesionado, por lo difícil que le resultaría probar el ilícito. Además, la equidad exige que los casos de menoscabo de la intimidad hagan prevalecer los daños ocasionados sobre la culpa. Por ello se dice que en materia de violaciones a la intimidad, la intromisión debe ser arbitraria y no necesariamente dolosa o culposa, para que se admita la reparación del daño. Y la intromisión es arbitraria en materia informática cuando se violan los principios fundamentales consagrados en las leyes de datos (Infra, págs. 162 y siguientes).

En el aspecto extracontractual, la gestión de bancos de datos puede ocasionar daños patrimoniales (frustración de ganancias legítimas, pérdida de un chance de

naturaleza comercial, profesional o laboral) o morales sean estos subjetivos u objetivos (lesión del honor).

En términos generales, la gestión de bancos de datos se viene considerando una actividad peligrosa, a partir del momento en el cual la actividad informática ha hecho posible almacenar información en proporciones no previsibles en el pasado y su procesamiento de manera sistemática y completa, además de su difusión en ámbitos ilimitados. Esto va a generar un potencial peligro por la posibilidad de difundir información distorsionada sobre las personas, de tal forma que el sólo hecho de que se conserve información incorrecta en el banco de datos crea un peligro potencial. Ello implica que la actividad no puede considerarse peligrosa por su naturaleza o por su almacenamiento, sino más bien por la forma de su realización, o sea por la utilización de la informática. Por ello, la susceptibilidad de dañar de la gestión de bancos de datos, determina que se le señale como una actividad peligrosa.

La gestión de bancos de datos como actividad potencialmente peligrosa puede causar una lesión, la cual si bien puede afectar diversos bienes e intereses jurídicos, lo cierto es que el menoscabo del derecho a la intimidad, va a ser la mayor preocupación para los legisladores de nuestro tiempo, como señalaremos con mayor amplitud en el capítulo siguiente.

D. Limitación o exoneración de la responsabilidad del banco en función de su naturaleza objetiva o subjetiva.

Finalmente debemos referirnos al interesante y discutido punto de una posible liberación de la responsabilidad del banco y sobre la calificación de su responsabilidad como objetiva o subjetiva, en cuanto a los hechos informáticos que su actividad provoca.

Hay quienes proponen la aplicación del régimen de la responsabilidad por el hecho de las cosas, aunque vale advertir que dicha teoria no es de aceptación unánime, ya que autores como Bustamante Alsina (Bustamante, 1992b: 244) rechazan el hecho de que los computadores o elementos magnéticos sean cosas peligrosas que dañen por sí mismas, sino más bien instrumentos que el hombre maneja según su voluntad. Sin embargo, quienes acogen esta teoría señalan que si bien la informática no es, como lo señala Borda (Borda, 1990: 333), en *strictu sensu* una cosa, es al menos una forma de energía y, por lo tanto, le debe ser aplicado el régimen de las cosas. Por tal razón pueden proponerse alguna de las teorías siguientes:

(1) Que la responsabilidad del banco en estos casos es objetiva y que el operador sólo puede, liberarse por la culpa de la víctima, de un tercero por el cual no debe responder o por caso fortuito o fuerza mayor ajena a la cosa. Tal afirmación parte de la premisa de que la informática es una cosa riesgosa. Nuestra legislación adopta este criterio objetivo tratándose de los daños causados por las cosas riesgosas en los artículos 1650, 1652 y concordantes del Código Civil, aunque debe advertirse que los mismos no guardan relación con la actividad informática. Otras legislaciones en cambio si lo hacen, como es el caso de la argentina, que tratándose de la actividad riesgosa en que consiste la informática bancaria, señala que el responsable será quien ejerza la actividad

riesgosa, o sea el banco, en relación adecuada de causalidad con el daño inferido, aun a través de sus dependientes (los empleados del banco), en razón de la denominada responsabilidad refleja.

En estos casos el banco resulta un legitimado pasivo, puesto que es el mismo quien introduce el riesgo de su actividad en la sociedad.

(2) Que la responsabilidad del banco es subjetiva, según se infiere de las opiniones que entre otros aporta Bustamante Alsina, ya que no puede establecerse la existencia de responsabilidad si no se prueba que el daño es el resultado de culpa o dolo del operador del sistema, o sea el banco, ya que en todo caso será este último, quien por su voluntad y acción determine el funcionamiento del computador.

(3) Que pudiendo ser el computador operado por un hombre o en forma automática, en el primer supuesto estaremos frente a una responsabilidad de tendencia subjetiva y en el segundo objetiva.

En adición a lo anterior se agrega el hecho de que la responsabilidad en este caso, siendo extracontractual, puede reputarse directa por el hecho del operador sobre el computador, con lo cual será el operador quien deberá acreditar la ausencia de culpabilidad, ya que la misma se presumirá. Si ello es así, entonces el hecho de que se compruebe la existencia o ausencia de culpabilidad resultará intranscendente, imponiéndose la presunción de culpa. Esto además de las dificultades que implica la probanza de la ausencia de culpa.

Por lo anterior, resulta que el banco para liberarse de responsabilidad en estos casos, deberá demostrar la culpa de la víctima (el cliente) o de un tercero-de quien no debe responder o por caso fortuito o fuerza mayor ajena a la cosa, o sea en todo caso,

como resultaría del hecho de que la responsabilidad se definiera siempre como objetiva. Esto último implica que el banco podrá exonerarse de responsabilidad si resulta que fue el cliente el culpable del daño infringido a su patrimonio o al patrimonio de un tercero. Y es que el cliente esta en capacidad de utilizar de forma inadecuada los mecanismos de acceso al sistema informático que el banco le proporciona y causar con ello daños. Inclusive puede ocurrir que no sea directamente el cliente sino un tercero que reciba sus instrucciones o que sencillamente pueda disponer de los mecanismos de acceso y este en capacidad de llevar a cabo en su nombre una determinada transacción, ejecutando un acto dañoso.

En términos generales, la doctrina considera que es eximente de responsabilidad objetiva, incluida la actividad riesgosa, la incidencia de una causa ajena al riesgo o vicio (caso fortuito). No puede el banco, sin embargo, liberarse de responsabilidad sobre la base de los llamados riesgos del desarrollo, o sea los daños que no pudieron ser previstos al tiempo en que la actividad riesgosa se inició, por la falta de los conocimientos técnicos que impedían advertir su peligrosidad. Lo anterior es así puesto que a pesar del relativamente reciente desarrollo a gran escala de la informática, la ciencia informática y su aplicación a la actividad bancaria, no permiten hoy en día definir con absoluta certeza, los riesgos que la misma implica para los intereses de sus usuarios.

Como señala Borda: "....podrá discutirse si se trata de una actividad riesgosa (...) o de una energía riesgosa, pero que existe riesgo me parece indudable..."(Borda, 1990: 335).

La responsabilidad informática y los perjuicios que la misma causa tratándose de una responsabilidad objetiva causada por cosas que actúan activamente, resulta encuadrada en la legislación argentina, según autores de ese país (Messina, 1989: 130),

específicamente en el artículo 1113 del Código Civil. No obstante lo cual, se opina que dicha responsabilidad debería ser considerada en forma más adecuada dentro del concepto de actividad riesgosa, la cual no tiene sistema normativo en la legislación argentina ni se encuentra establecido tampoco con la claridad y amplitud deseada en la panameña.

La naturaleza de la responsabilidad del banco, en estos casos, resulta para algunos tan discutida, que inclusive se ha propuesto una clasificación de la responsabilidad del banco como proveedor de los servicios informáticos así:

1. La responsabilidad que surge del mal funcionamiento del equipo.
2. La responsabilidad que tiene que ver con los medios de acceso.
3. La responsabilidad relacionada con el incumplimiento o el cumplimiento tardío de órdenes.
4. La responsabilidad por negligencia o descuido en el trámite de la operación.
5. La responsabilidad objetiva o sin culpa.

III. Elementos de la responsabilidad.

A. La antijuridicidad.

Habiendo disposiciones legales y contractuales que obligan al banco a brindar una información cierta a su cliente y a la vez a no revelar esta información a ninguna persona no autorizada por la Ley o por el propio cliente, la infracción de estos deberes,

ya sea porque el sistema informático operado por el banco o en nombre del banco no pueda suministrar la información, la suministre de forma incompleta o incorrecta o aun permita que la información electrónicamente almacenada sea sustraída de su memoria por empleados del propio banco o por otros terceros no autorizados y la misma sea revelada, todo ello ocasionado por la inobservancia del banco de fundamentales deberes u obligaciones de naturaleza técnica, provocará que éste incurra en responsabilidad legal contractual para con su cliente y aún extracontractual cuando las faltas del banco afecten negativamente a terceros, o lo que es lo mismo incurra en un acto desaprobado por el ordenamiento jurídico, es decir de antijuridicidad.

B. El daño.

El factor daño viene dado por la lesión que el banco causa cuando como resultado del procesamiento electrónico de la información se produce una lesión al patrimonio (daño patrimonial), a la intimidad y aun al honor (daño moral) de sus clientes o se le priva del disfrute de los derechos o de la expectativa lícita a continuar disfrutando de los derechos sobre tales bienes jurídicos protegidos (Zannoni, 1993: 25).

En este aspecto se discute si el denominado daño informático comprende sólo el tratamiento ilícito de la denominada información nominativa, o sea los relativos a la identificación de las personas (Infra, pág. 180) o se extiende también a los datos no nominativos, pero igualmente deficientes o erróneos. Nosotros nos inclinamos a pensar igual que Parellada, pues consideramos que el daño informático debe incluir el

tratamiento ilícito de otro tipo de información diferente a aquella que sólo refleja la identidad de las personas, tal como la información sobre el patrimonio personal, sobre el cumplimiento de las obligaciones, etc. Es un hecho que la información que los bancos manejan sobre sus clientes, no es sólo aquella que permite su identificación personal, la cual cobra hoy mayor importancia, por la lucha continua contra el uso indebido de los servicios bancarios para actividades criminales, sino también aquella que hace relación con sus deudas, sus ingresos, sus relaciones laborales y en general todo aquello que resulte importante para la realización de las operaciones bancarias sean estas activas, pasivas o neutras.

Se ha esbozado una clasificación de los daños informáticos sobre la base de si el daño proviene de la información tratada o de la cosa, sea el *hardware* o el *software*. Para los efectos de este estudio nos interesa la primera clasificación y aquella que tiene que ver con el daño causado por el uso de un *software* deficiente, ya que en el caso del daño causado directamente por el *hardware*, este atañe más bien a aquellas lesiones corporales o sicológicas que la máquina puede ocasionar a una persona.

En cuanto al daño proveniente de la información tratada electrónicamente, debemos mencionar que el mismo guarda relación con la trascendencia de la información para la persona a quien la misma concierne o con el producido a quien toma decisiones sobre la base de los datos a los que tiene acceso.

El mencionado daño es también el originado en los datos que se ingresan al computador, lo que se conoce como el *input* y que afectan más que nada a aquellos con quienes se relaciona la información, es decir estamos hablando de los datos nominativos y de los no nominativos pero siempre personales; o, los datos que salen del computador, o sea lo que se conoce como el *output* y que afectan a las personas que reciben una

orientación y que toman decisiones sobre la base de dichos datos. Tal es el caso de aquellos que realizan operaciones de bolsa sobre la base de datos bancarios computarizados sobre el estado financiero de las empresas que cotizan acciones u otros títulos en la bolsa. Debe tenerse en cuenta que la causa del daño la constituye el ingreso de la información al computador, sin que interesen otros elementos relacionados con el mismo.

Tratándose del daño causado por un *software* deficiente, la responsabilidad del banco surgiría para con su cliente con el cual mantiene una relación contractual, sin embargo cuando se trata de un tercero, el controlador del banco de datos podría alegar que el hecho no es propio sino del programa, o sea de la cosa. En este caso el mismo asumiría una responsabilidad en la medida en la que la legislación reconociera su responsabilidad como dueño o guardián de la misma, lo cual no ocurre en nuestro país.

C. Nexo de causalidad.

Por otra parte, para que surja responsabilidad para el banco se necesita que exista un nexo causal entre el actuar del banco como controlador de un sistema informático y el daño que el uso por parte del banco, incluyendo su personal o terceros que acceden al sistema, causen al patrimonio del cliente que el banco maneja o a su intimidad, honor o identidad personal. Es decir se requiere la existencia de un nexo de causalidad entre el actuar del banco y el daño ocasionado. En otras palabras, que el

daño haya sido causado por la información como producto del procesamiento de los datos.

La relación de causalidad permitirá revelar al autor del daño y así atribuir la responsabilidad y establecer la extensión del resarcimiento. Este último aspecto cobra especial relevancia si consideramos un criterio subjetivo de responsabilidad, pues debe establecerse si la misma se extiende a los daños que sean consecuencia inmediata o mediata previsible del daño o también a los imprevisibles, si estamos frente a una acción dolosa. Cabe señalar que, en muchos casos, las consecuencias inmediatas del ilícito informático no serán necesariamente daños patrimoniales de trascendencia económica, sino por su conexión con otro hecho como las relaciones jurídicas patrimoniales del titular de dicha información, por lo que la consecuencia será mediata. Así se produce lo que se conoce como un daño patrimonial indirecto, porque aún cuando los bienes jurídicos afectados son de principio, inmateriales, al distorsionarse la personalidad o identidad de un individuo, se ocasiona un efecto negativo en el plano patrimonial.

No obstante lo anterior, es evidente que la relación de causalidad puede interrumpirse si se evidencia que el daño producido tuvo su origen en el actuar del propio cliente que proporcionó información incorrecta al banco o que por su actuar negligente permitió que un tercero penetrara el sistema informático, sin que el banco tuviese tiempo para adoptar las medidas a su alcance para impedir tal acceso. Igualmente se interrumpirá el nexo causal ante un caso fortuito o fuerza mayor, aunque aún en estos casos podría haber cierta responsabilidad para el banco, si éste no adopta las medidas técnicamente recomendables para evitar que este caso fortuito o de fuerza mayor afecte la información electrónicamente almacenada.

D. Factores de atribución.

Para que el banco asuma responsabilidad, siguiendo un criterio subjetivo, se requiere que el mismo o su personal, hayan actuado en forma culposa o dolosa en el procesamiento y almacenamiento de la información. Si bien podría hacerse alusión a una responsabilidad dimanante del factor riesgo, por efecto de que es el banco el que al optar por el almacenamiento y procesamiento electrónico de la información, a creado una situación susceptible de causar daños a sus clientes, nuestra legislación no reconoce aun, como ya afirmamos (Supra, pág.80), que de la actividad bancaria y menos de la informática se pueda deducir una responsabilidad objetiva.

IV. Obligaciones especiales de los bancos frente a sus clientes en razón del hecho informático.

El hecho de que los bancos utilicen la informática como instrumento adecuado para el mejor desenvolvimiento de sus operaciones y una mejor prestación de sus servicios, implica el cumplimiento más riguroso de ciertos deberes que por efectos de la Ley deben asumir y también el cumplimiento de nuevas obligaciones que dimanan precisamente del uso de la nueva tecnología informática.

A. Obligaciones Legales.

Como ya advertimos, la responsabilidad que surge para el banco al causar algún daño a sus clientes, en razón de los hechos informáticos que dentro de la actividad bancaria se suceden, es de naturaleza contractual. Por tal razón, debemos analizar en primer lugar las obligaciones de los bancos que guardan relación directa con el hecho de que éstos recurran a la tecnología informática en el procesamiento de la información de sus clientes, es decir aquellas que inciden muy especialmente en su forma de almacenar y ordenar la información que reciben. Entre estas obligaciones tenemos la de rendir cuentas adecuadas a sus clientes sobre las operaciones y la de mantener reserva frente a terceros sobre dichas obligaciones.

1. Obligación de rendir cuentas.

Esta obligación de rendimiento de cuentas tiene fundamento en diversas disposiciones legales que contemplan las obligaciones de los comerciantes en general y es un hecho que como ya advertimos (Supra, pág. 44), los bancos son comerciantes para todos los efectos legales. Entre estas disposiciones tenemos al artículo 34 del Código de Comercio, cuyo texto expresa:

Los comerciantes contraen, por el hecho de serlo, la obligación de someterse a las disposiciones de la ley mercantil; y están especialmente obligados:

...
4° A llevar contabilidad mercantil y conservar la correspondencia y libros que tengan relación con su giro;

5° A rendir cuentas según lo dicho en el artículo 96.

A su vez el artículo 96 del Código de Comercio expresa:

> Es obligatorio para todo comerciante la presentación de cuentas cuando las solicite el interesado. Estas han de ser conformes con los asientos de los libros de quien las rinde y debidamente comprobadas.

Sin embargo, los bancos también son proveedores de servicios, razón por la cual también les resultan aplicables las disposiciones vigentes para la defensa de los consumidores, puesto que sus clientes resultan consumidores de servicios bancarios. Por lo tanto, quedan sometidos a lo dispuesto en el artículo 31 de la Ley 29 de 1996, la cual entre otras obligaciones inherentes al proveedor de servicios, incluye en su numeral séptimo, la de mantener informado al consumidor sobre la evolución o el estado en que se encuentre la gestión respectiva, en el caso de la prestación de servicios.

Lo anterior implica que el banco asume la responsabilidad primordial de informar a su cliente de forma veraz sobre la evolución y el estado de sus asuntos, para cuyos efectos deberá llevar una adecuada contabilidad de sus operaciones, de forma tal que cuando el cliente así lo solicite según los términos y condiciones de los contratos celebrados, el banco pueda proporcionarle el saldo de su cuenta o en términos generales el estado correcto de sus negocios. Esta obligación resulta aún mayor si se toma en cuenta que en la mayoría de los casos, el banco asume el control de un patrimonio que no le pertenece y que únicamente le es entregado sobre la base de una relación de extrema confianza.

La utilización de la informática por parte de las entidades bancarias permite agilizar el cumplimiento de este deber de rendimiento de cuentas, sin embargo conlleva igualmente ciertos riesgos relacionados principalmente con la vulnerabilidad de los sistemas a la actuación dolosa o culposa de los funcionarios bancarios o la intromisión no autorizada de terceros, que en ambos casos puede causar la pérdida o alteración de la información; igualmente la posibilidad de desperfectos en los equipos o los sistemas informáticos pueden ocasionar las mismas anomalías. Todos estos hechos implicarán que el banco no pueda cumplir con su deber de rendimiento de cuentas, y causar una daño al cliente al privarlo del derecho que tiene de conocer el estado de sus cuentas y negocios que mantiene con el banco, es así que más que una lesión a un bien jurídico específico, lo que aquí se trata es de una lesión a un interés jurídico, el cual viene representado por el derecho que tiene el cliente de conocer la información que a él le concierne. Por tal razón, en ciertos casos como el relativo a la transferencia electrónica de fondos, el derecho comparado exige a los bancos el cumplimiento de ciertas obligaciones para con sus clientes. Es así como en la *Electronic Fund Transfers Act* de 1978 y que fuese promulgada para la protección de los consumidores estadounidenses, se imponga a las entidades bancarias, entre otras, las siguientes obligaciones:

1. Brindar a los clientes la información necesaria sobre la responsabilidad del banco por transferencias no autorizadas y otras condiciones inherentes a las partes de una transferencia electrónica de fondos.

2. Documentar por escrito cualquier operación que tenga por inicio una terminal electrónica con detalles tales como los montos, el tipo de transferencia, identificación de las cuentas, saldos, fechas, etc.

3. Poner a disposición del cliente de manera regular, un resumen o histórico de las operaciones efectuadas mediante transferencia electrónica de fondos.

Esta obligación de seguridad que asume el banco como responsabilidad contractual y que se refleja en la obligación de proveer una información correcta es, en todo caso, una obligación de resultado.

2. Obligación de reserva.

La otra obligación de relevancia que surge para el banco es la de mantener reserva en cuanto a la información que recibe de su cliente, sea esta de índole financiera, personal o de cualquier otra naturaleza. Tal obligación que también es contractual y de resultado, constituye una institución en la actividad bancaria y es comúnmente denominada secreto bancario. Tal institución tiene un reconocimiento legal, ya sea de forma expresa, como sucede con las cuentas cifradas (Ley 18 de 1959) o el fideicomiso (Ley 1 de 1984), ya sea como parte de una figura genérica como en el caso de los delitos contra la inviolabilidad del secreto y específicamente en lo que se refiere al secreto profesional (artículo 170 del Código Penal) o en forma analógica por aplicación de lo dispuesto en el artículo 101 del Decreto de Gabinete 238 de 2 de julio de 1970.

En la utilización de los sistemas electrónicos de procesamiento de datos tiene especial relevancia, el deber de reserva, puesto que gran parte de la información que los bancos tratan a través de estos sistemas constituye objeto material de dicho deber, tal es el caso de los saldos de los clientes, los límites de sobregiro y los detalles de las

transacciones. Además resulta creciente el número de personas que sin ser empleados bancarios tienen acceso a dicha información en razón de los servicios profesionales que prestan al banco, ya sea como consultores o técnicos independientes en materia informática o por haber contratado el banco una empresa para que le preste en forma parcial o total el servicio de procesamiento electrónico de sus datos, tal y como sucede con el novedoso contrato de *outsoursing*, y esto sin contar con el desarrollo que ha tenido la transferencia electrónica de fondos a través de los llamados cajeros automáticos y los puestos de venta.

Sin embargo desde el punto de vista legislativo, la tutela del derecho a la intimidad eclipsa en cierto sentido -sobre todo en las normativas más desarrolladas- la tutela de la reserva o secreto bancario, considerando el carácter más restringido de este último, así como el desarrollo conceptual del derecho a la intimidad, que tal y como veremos (Infra, pág. 144 a 145), se define en la actualidad como un derecho de control sobre la información que concierne a una persona, con lo cual el derecho de autorizar la revelación de la información financiera se convierte en la contraparte del deber de no revelarla. Esto trae como implicación directa, una regulación única para tutelar tanto los derechos como los deberes sobre la información financiera de las personas, sean éstas naturales o jurídicas.

La información que almacenan los bancos de datos de las entidades bancarias es susceptible de ser utilizada para clasificar a su clientela en función de sus características y antecedentes comerciales, escolares, médicos, profesionales, financieros, etc. Por esta razón se legisla para establecer las normas que regulen los bancos de datos con relación a la clase de información que se puede almacenar, a su actualización, a los fines para los que se puede utilizar y los derechos que tienen los clientes cuya información es

almacenada. Según Peña Castrillón: "esto conduce a que la banca tenga que observar el secreto de la información que procesa más allá de un deber profesional tradicionalmente reconocido y tutelado y considerado, también como la carga y cuidado que le impone la protección de un nuevo derecho, el derecho a la intimidad" (Peña, 1979: 54).

Comparando el peligro de revelación no autorizada de información confidencial en los sistemas de procesamiento electrónico de datos frente a los sistemas manuales, se concluye que en los primeros se pueden extraer cantidades mucho más grandes de información en forma más conveniente y procesable sin que quede huella de que ha habido acceso no autorizado.

De esta forma se infiere que el incumplimiento del deber de reserva provoca una lesión directa de bienes jurídicos como la intimidad y también el secreto en su ámbito bancario, sin perjuicio de que indirectamente puedan afectarse otros tales como el honor y el patrimonio.

En estos casos, o sea la revelación de información sensible, en este caso de naturaleza bancaria, la cual ha sido electrónicamente tratada, no cabe invocar la *exceptio* veritatis, o sea si la misma es verdadera o errónea. La sola divulgación de la misma mediando la culpa del controlador del banco de datos, en los regímenes de responsabilidad subjetiva o el sólo hecho de la divulgación, en los regímenes de responsabilidad objetiva, es motivo suficiente para que surja una responsabilidad a cargo del controlador del banco de datos, en nuestro caso, el banco.

B. Obligaciones Técnicas.

Como ya dijimos, la responsabilidad de los bancos es una responsabilidad profesional en todos los ámbitos de su actividad, puesto que se entiende que los banqueros tienen un conocimiento sobre la misma que supera los conocimientos de cualquier persona común. Así cuando los bancos utilizan las facilidades informáticas para la realización de sus operaciones, la informática se convierte en un tema que entra dentro de la esfera de conocimientos especializados que se presume dominan los banqueros, ya que al controlar éstos de forma directa su propio sistema de informática o al contratar un servicio externo, los mismos asumen la responsabilidad de que el mismo funcione de tal manera que no cause ningún daño a sus clientes o terceros, asumiendo las consecuencias perjudiciales que las fallas en dicho sistema cause, producto de un manejo técnicamente deficiente de los mismos o de la omisión en el seguimiento de las prácticas preventivas o correctivas de los bienes que componen dicho sistema.

Entiéndase que hechos como la sustracción de información sensible sobre los clientes de una banco, puede comprometer la responsabilidad de este último, si el mismo no ha observado las reglas de seguridad necesarias para que tal sustracción no se produjera. En este caso se considera que la culpa del banco es indiscutible en la producción del daño.

Los sistemas informáticos comportan el uso de dos componentes fundamentales, el uso de un equipo o "*hardware*" y un programa adecuado o "*software*" con el fin de obtener los resultados esperados.

El *software* es el concepto universalmente aceptado para individualizar los elementos de identificación y análisis de los problemas que deben ser resueltos por las computadoras, el programa de computación que resulta del análisis de tales elementos y el material de apoyo (Correa et al., 1987: 55). La Organización Mundial de la Propiedad Intelectual lo define como: "...además del propio programa de ordenador, la descripción detallada del programa que determina el conjunto de instrucciones que constituyen el correspondiente programa y todos los tipos de material de soporte creados para que contribuyan a la comprensión o aplicación de un programa de ordenador, tales como las instrucciones para el usuario (Delpiazzo, 1990: 371). Sin embargo, dicho concepto ha sido casi siempre asociado a su principal componente, es decir el programa de computación. La *Public Law* 96-517 de diciembre de 1980 de los Estados Unidos de América señala que el programa de computación es: "un conjunto de afirmaciones o instrucciones para ser usadas directa o indirectamente en un ordenador a fin de obtener un resultado determinado" (Delpiazzo, 1990: 56). Una definición bastante completa es la sugerida por la Organización Mundial para la Protección de la Propiedad Intelectual, la cual señala que el programa de computación es:

> ...una expresión (organizada, estructurada) de un conjunto (secuencia, combinación) de instrucciones (afirmaciones, órdenes) en cualquier lenguaje o anotación (de alto nivel, intermedio o de ensamblaje, o de máquina) en cualquier medio (magnético, óptico, eléctrico, en papel o en cintas, discos, "chips", circuitos, ROM) apto para lograr que una computadora (directa o indirectamente, con datos o sin ellos) o un robot (máquina de procesamiento de información) realice un trabajo (o ejecute una función específica). (Delpiazzo, 1990: 57).

Por su parte la Ley 15 de 8 de agosto de 1994, por la cual se aprueba la Ley sobre el derecho de autor y derechos conexos y se dictan otras disposiciones, en su artículo 2 numeral 20, define los programas de ordenador como:

> Conjunto de instrucciones expresadas mediante palabras, códigos, planes o cualquier otra forma que, al ser incorporados en un dispositivo de lectura automatizada, es capaz de hacer que un ordenador, un aparato electrónico o similar capaz de elaborar informaciones, ejecute determinada tarea u obtenga determinado resultado.

El *software* puede clasificarse en programas de base, los cuales controlan el funcionamiento interno de la computadora y del equipo periférico y permiten la comunicación con el usuario; y, programas de aplicación, o sea aquellos que permiten la utilización efectiva del ordenador y por lo tanto la realización de las operaciones específicas que el usuario requiere. Estos últimos programas, contenidos en disquetes o discos duros, pueden ser introducidos en la memoria viva de la computadora y borrados cuando lo requiera el usuario.

También pueden distinguirse los *softwares* estándar, o sea los programas definidos, estables y dirigidos al mercado general, y no a un usuario particular; los denominados a medida, que implican la elaboración integral de nuevos programas, o la modificación sustancial de programas existentes para cubrir las necesidades específicas de un usuario; y, el adaptado, que consiste en un programa estándar, que se modifica para acomodarlo a las necesidades de un cliente.

Por otra parte, el *hardware* "comprende la totalidad de dispositivos y elementos mecánicos, magnéticos, eléctricos y electrónicos en una instalación de procesamiento de

datos" (Delpiazzo, 1990: 326), es decir lo que comúnmente denominamos el equipo o parte o soporte físico, incluyendo el procesador central o *CPU* (*Central Processing Unit* o Unidad Central de Procesamiento) y todos los componentes que giran a su alrededor, también denominados periféricos.

Pues bien, cuando el banco selecciona en forma desacertada el *hardware* o *software* que va a utilizar en el manejo de la información de sus clientes y en la prestación de sus servicios a éstos, o no previene o da mantenimiento adecuado a tales componentes, puede causar un daño a éstos, ya que las fallas en el sistema informático causarán una imposibilidad de realizar adecuadamente sus operaciones y determinará el no cumplimiento adecuado de sus obligaciones comunes y aquéllas más estrechamente ligadas al uso de la informática, tales como la de rendir cuentas y la de reserva de la información, sobre todo las de sus clientes.

Es así que los bancos deben asumir una serie de obligaciones, que nosotros hemos denominados de carácter técnico, y con las cuales deben prevenir o evitar los daños que puedan ocasionar a sus clientes por el mal funcionamiento del sistema informático, pues de lo contrario sería evidente el surgimiento de una responsabilidad que inclusive podría ser identificada como culpa por abstención (Mazeud, 1977: 221 a 222). Y es que el sistema informático no esta exento de riesgos de funcionamiento que deben ser prevenidos o evitados. Así los incendios, perturbaciones técnicas, actividades criminales, riesgos ambientales relacionados con la ubicación, desastres naturales, fallas en el suministro de energía, errores de personal no capacitado (Eckstein, 1989: 18-35), son algunos de los riesgos que deben ser atendidos con medidas como las que detallaremos a continuación, más que nada porque como bien se dice: es preferible evitar el daño que resarcir el producido.

Por otra parte, hay quienes definen como áreas de riesgo del centro informático de un banco aquellas relativas a las facilidades, personal, seguridad y archivo, documentación y datos (Rivera, 1987: 173). Aunque para otros se trata tan sólo de medidas preventivas, clasificables según su relación con el personal, las relacionadas con el *hardware*, con los procedimientos administrativos y las meramente jurídicas (Jijena, 1992: 123).

Para nosotros, entre los deberes de naturaleza técnica y de orden práctico, que el banco debe observar, se pueden citar:

1. La existencia de procedimientos adecuados de control y seguridad del sistema informático para proteger al banco.

Los niveles de control pueden ser varios según el grado de riesgo y el impacto de la pérdida (o revelación) para la Institución. Tecnológicamente pueden incluirse controles tales como: la criptografía o la encripción, procedimiento mediante el cual el texto puro se convierte en hileras encriptadas de símbolos sin sentido (ciframiento de datos); el uso de códigos de autenticación de mensajes, en el cual se designa un código particular para evitar la alteración no autorizada de transacciones con datos electrónicos durante su transmisión o almacenamiento (protección efectiva contra las personas externas que pretendan incurrir en conductas responsables) y el uso de *software* de seguridad diseñado para restringir el acceso a los datos, archivos, programas servicios y comandos del sistema de computación. Tales sistemas pueden controlar el acceso por el usuario (uso de *passwords*), por la transacción y por el terminal. De tal forma las violaciones e intentos de violación del sistema de seguridad pueden ser informados y/o rastreados.

Los anteriores sistemas deben incluir la existencia de niveles de acceso a la información almacenada en el sistema, de tal forma que no todos los funcionarios del banco puedan acceder a toda la información e inclusive para que sólo ciertos funcionarios, conforme a su nivel de jerarquía, puedan realizar u ordenar al sistema, la validación de determinadas operaciones o la realización de determinadas acciones en general (acceso sólo para lectura, acceso sólo para escritura, actualizaciones y otras). Rivera sugiere inclusive que "en el uso de terminales remotas, es conveniente hacer un uso apropiado del sistema de claves que evite que sean copiadas o adivinadas con facilidad. Si es necesario se debe transmitir la información criptografiada" (Rivera, 1987: 185).

Entre los sistemas existentes es preciso resaltar el sistema TRASEC (*transaction Security*), el cual es un sistema de seguridad estándar para la transferencia electrónica de fondos entre los clientes empresariales y las instituciones financieras belgas (Van Heurk, 1989: 23). Este sistema fue creado por el Centro para la Investigación Interbancaria en Informática. Dicho sistema tiene por finalidad el detectar los intentos de fraude durante la transferencia entre una compañía y su banco. Cuando el banco recibe datos autenticados por una firma electrónica, activa las rutinas de seguridad que, automática y rápidamente, realizan las verificaciones necesarias antes de procesar los datos.

En adición a los procedimientos anteriores, hoy en día, existe la posibilidad de identificación de los usuarios y por lo tanto de limitar su acceso al computador, utilizando aspectos tales como: sus huellas digitales, la geometría de su mano, el análisis de la huella vocal e inclusive su firma. Y no es que un banco deba adoptar toda esta sofisticada y por lo tanto sumamente costosa tecnología, pero es un

hecho que el mismo no podrá argüir que la tecnología no le ofrece los recursos para brindar a sus clientes la protección que su información merece.

En el aspecto físico debe tenerse en cuenta que el acceso al área del centro de cómputo debe ser restringida, preferiblemente mediante sistemas electrónicos de identificación del personal o terceros autorizados para el acceso al local.

2. La creación de los llamados *back-ups* o copias periódicas de toda la información.

Estas copias deben estar claramente identificadas y almacenadas en un lugar seguro. Esto último implica que los *back-ups* deben ubicarse en lugares distantes del centro de cómputo y en instalaciones que reúnan las condiciones con que cuente el propio centro de cómputo.

3. La ejecución de un mantenimiento preventivo tanto del *hardware* como del *software*.

4. La selección de un software adecuado, pues los errores que éste incluye pueden ser varios.

Los errores se presentan, típica y frecuentemente, durante la entrada de datos y el desarrollo y modificación de programas. Pueden también surgir errores durante el proceso de diseño del sistema, durante los procedimientos domésticos de los sistemas de rutina y cuando se utilizan programas especiales para corregir otros errores. La causa de tales errores es generalmente una falla humana, siendo infrecuente que los errores se produzcan por falla de los componentes internos electrónicos o mecánicos. Los errores pueden venir también en los paquetes de software, cuando estos resultan adaptados para que se ajusten a las necesidades de un usuario determinado. Por lo tanto, en muchos casos los bancos prefieren comprar *softwares* estándar para reducir al mínimo los cambios.

5. La existencia de sistemas de control y producción de informes destinados a la prevención o detección de fraudes.

Para ésto resulta importante identificar los puntos vulnerables de cada sistema. Los registros y programas críticos deben ser especialmente protegidos contra cambios no autorizados. El personal que labora en las áreas críticas debe estar correctamente capacitado y sus funciones deber estar segregadas en forma adecuada.

Algunas medidas que deberían adoptar los bancos serían: controles de entrada de datos, la instalación de dispositivos de seguridad para impedir el acceso no autorizado al equipo de computación y de claves (passwords) para restringir el acceso a los programas y datos del computador.

6. La existencia de planes de contingencia mediante los cuales las entidades bancarias puedan reducir el impacto de problemas operacionales previsibles.

Los planes de contingencia deben ser una prolongación del sistema de control interno y de seguridad física de un banco. Deben incluir disposiciones para la continuación de las operaciones y la recuperación cuando los sistemas del banco se interrumpan, o sea medidas para proteger los archivos de datos críticos, de *software* y de *hardware*, al igual que medios alternativos para procesar la información, o lo que se conoce como un sistema de respaldo.

Estos planes de contingencia deben probarse periódicamente para constatar su eficacia. Si el banco se sirve de un proveedor externo de servicios de procesamiento electrónico de datos, debe asegurarse que éste tenga un plan de contingencia propio.

Algunos (Superintendencia, 1990: 41) hablan también de las denominadas medidas de contención, las cuales deber estar diseñadas para detectar y limitar los efectos de los hechos que se desvíen de los controles preventivos y que amenacen las

operaciones del banco. Estas medidas deberían incluir la doble capacidad de las redes de computación y telecomunicaciones para cubrir el riesgo de daños en los equipos, los procedimientos de reconciliación para detectar errores y en forma específica la existencia de un seguro contra pérdidas imputables a fraude por parte de los empleados, a costos de reposición de datos y a destrucción de *software* o de equipos.

Rafael Rivera, quien vivió la experiencia del terremoto de México en 1985 y la forma en que se afrontó con éxito la reanudación rápida y efectiva de las operaciones informáticas del Banco Nacional Financiera de México, estima que los requerimientos de seguridad básicos para un centro de informática son los siguientes:

Respaldo local de todos los sistemas, aplicaciones, archivos clave y documentación.

Almacenamiento remoto de todo lo anterior.

Almacenamiento remoto en refugios subterráneos u otra instalación segura de las aplicaciones críticas.

Vigilancia armada para seguridad del centro de datos.

Equipo de detección de humo y fuego de todas las instalaciones.

Equipo de detección de fuego (el Halógeno es el mejor material).

Acceso controlado al centro de cómputo y otras instalaciones (Rivera, 1987: 199).

7. La adecuada supervisión e introducción de los controles básicos en los computadores personales, los microcomputadores y los equipos de computación para el usuario final, en vista de la cada vez mayor utilización de estos sistemas informáticos,

principalmente reflejada en el uso de cajeros automáticos (*ATM*) y puntos de venta (*POS*).

Cabe advertir nuevamente, que estas herramientas permiten realizar el procesamiento electrónico de datos fuera de las áreas comúnmente utilizadas para el control central de estas operaciones. El problema peculiar que muchas veces se presenta con estas nuevas herramientas, radica en el hecho de que el uso de las mismas no va a la par con el establecimiento de los correspondientes controles, lo cual hace a los mismos susceptibles de una mayor incidencia en la pérdida o alteración de la información o del propio *software* y consecuentemente en el mal funcionamiento del sistema informático de la entidad.

8. El cuidadoso diseño y ubicación del centro de informática es imprescindible, además debe contar con instalaciones apropiadas.

Se recomiendan entre otros aspectos, que los centros de cómputo no estén situados en áreas bajas ni tengan ventanas, además deben incluir un sistema propio de aire acondicionado con especificaciones adecuadas para evitar accidentes que ocasionen un daño al equipo, incluyendo un posible recalentamiento; debe haber una fuente de energía permanente, con sistemas alternos a los públicos y con equipos *UPS* (reguladores de voltaje y fuentes alternas de energía, generalmente mediante una batería), que eviten daños por los cambios de voltaje repentinos; debe haber un sistema de iluminación adecuado. Ésto es así, puesto que tales sistemas cuentan con un gran número de equipos independientes y de componentes de *software*, y la falla de cualquiera de ellos puede detener el sistema, de tal forma que si estos componentes se encuentran concentrados en un solo sitio o en pocos sitios, se incrementa el riesgo de accidentes. Además, la construcción de las instalaciones del centro de cómputo debe

incluir la utilización de materiales que minimicen el riesgo de incendios y la instalación de sistemas que controlen en sus inicios un conato de este siniestro.

9. La inclusión de un programa para la auditoría de los sistemas, el cual debe permitir revisar, controlar y probar los sistemas de control del procesamiento electrónico de datos, con el fin de garantizar su permanente efectividad y su continua relevancia para el sistema.

Los auditores internos y/o externos deben ejecutar un programa de pruebas de seguridad y de procedimientos de control, a fin de identificar lapsos en el control antes de que éstos pongan en peligro las operaciones bancarias. La frecuencia y profundidad de las pruebas de auditoría efectuadas en cualquier área, deben reflejar el nivel de riesgo para el banco, si los procedimientos de seguridad y control de dicha área fallan en un momento dado. Según Carreño, existen varias clases de auditajes que deben ejecutarse, tales como:

Evaluación de controles generales, revisión de seguridades físicas, auditoría al plan de contingencia, auditoría al área de operaciones del computador, auditoría para procedimientos de mantenimiento a sistemas y programas, auditoría al sistema operacional, entre otros.

10. La contratación de personal con idoneidad moral y técnica, lo cual resulta imprescindible para minimizar los riesgos relacionados con actos criminales y la comisión de errores en la operación y el mantenimiento del sistema informático.

En no pocos casos, resulta ser el propio personal del banco el responsable directo o cómplice en la comisión de actos tendientes a la destrucción o alteración de información electrónicamente almacenada, ya sea con la intención de obtener un

provecho económico o simplemente para perjudicar a la entidad bancaria. Las transferencias ilícitas de fondos de cuentas de clientes a cuentas controladas por empleados o por terceros asociados con éstos, resultan comunes. También la introducción de diversos tipos de virus (Infra pág. 186) con la intención de provocar alteraciones a los programas o *softwares* para sustraer fondos de los clientes o de las cuentas contables del propio banco, aunque en algunos casos tales virus pueden también tener el único propósito de trastornar el sistema y borrar o alterar información con la finalidad de provocar un perjuicio al banco.

La contratación de personal pobremente capacitado aumenta la posibilidad de que se comentan errores de programación o que aumenten los desperfectos en el *hardware*, con lo cual la prestación adecuada o continuada de los servicios puede resultar afectada y el incumplimiento de una responsabilidad *in eligendo*. Las constantes caídas del sistema o el mal funcionamiento de un equipo que no responde a una programación correcta serán frecuentes, sino se cuenta con un personal debidamente capacitado para responder a los requerimientos técnicos del sistema.

En atención a los anterior, lo expertos recomiendan mantener una adecuada política para la contratación del personal, de forma tal que éste labore según normas que tiendan a optimar sus labores y también una política de adiestramiento permanente.

11. La inclusión de programas antivirus o vacunas, para el combate de tipos específicos de virus, como aquellos a los que nos referimos anteriormente y sobre los cuales abundamos en detalles en el capítulo siguiente (Infra, pág. 186). Estos programas también ayudan a establecer la existencia de ciertas anomalías en los archivos gravados

del disco y más específicamente intentan evitar la entrada de un virus al sistema, su reproducción o el bloqueo de las instrucciones ilícitas.

V. La internacionalización del hecho informático bancario.

A. Consideraciones Generales.

En aquellos países que cuentan con una legislación sobre materia informática se incluyen normas reguladoras del denominado flujo de datos transfrontera o *transborder data flow*, el cual requiere en algunos casos hasta de permisos especiales. Ello porque la protección de los datos y sobre todo aquellos de carácter personal, ya forma parte del denominado Orden Jurídico Internacional.

En razón de lo anterior, resultan necesarias normas que tutelen la denominada información sensible (Infra, pág. 145 a 146), o sea aquella que puede afectar de forma más acentuada los intereses legítimos de las personas en cuanto a su intimidad, su patrimonio o su honor, siendo necesarias tales normas más que nada, cuando el país hacia el cual se transmite la información no tiene una legislación que tutele adecuadamente el derecho a la intimidad de las personas y principalmente a través de la protección de sus datos personales. Para no afectar la libertad de información (Infra, pág. 158), en algunos casos se ha recomendado que toda limitación al flujo de información, se fundamente en el principio de reciprocidad, es decir que se limite tal flujo de datos, siempre que el país de destino, no contemple una protección equivalente

a las ofrecidas en el país que origina la información. Esto sin contar el hecho de que los denominados datos sensibles (Infra, pág. 145 a 146), no pueden ser transmitidos libremente, toda vez que su recolección resulta restringida. Sin embargo, hay quienes señalan que aun ni esta reciprocidad es suficiente garantía, pues si los datos son transmitidos de un país protector a uno que si bien es protector, no previene en cuanto a la transmisión de éstos a un país no protector, tal situación permite la violación de la ley. Por ello se insiste en que se prohiba la transmisión de datos a países con una legislación demasiado permisiva en cuanto a la transmisión de datos transfrontera. Esto implica que si los estados no quieren ser objeto de un bloqueo informático en el futuro, deberán aprobar al más breve plazo, legislaciones para la protección de los datos informáticos, teniendo en cuenta los dos requisitos formales que la Comunidad Internacional esta considerando como necesarios para calificar a un país como protector del dato informático, o sea: la existencia de una ley de protección de datos y de una oficina de vigilancia que controle su aplicación.

En el ámbito de las relaciones internacionales se presentan generalmente dos corrientes antagónicas, a saber:

1. La desarrollada fundamentalmente por los países desarrollados, que reconoce la existencia del principio de libre circulación de los datos a lo interno del país y transfrontera, salvo en este último caso, por la aplicación del principio de reciprocidad. Esta corriente busca su sustento en el derecho individual a la información.

2. La que aflora en algunos países en vías de desarrollo, la cual propugna por la intervención del Estado para regular el flujo con medidas de carácter legal y técnico.

A nivel del derecho internacional, la Convención Internacional de las Telecomunicaciones de Torremolinos (Málaga, España) del 25 de octubre de 1973,

señaló que el flujo internacional de datos, debía efectuarse sin obstáculos ni interrupciones y conforme a condiciones de seguridad. Por su parte, la Convención para la protección de las personas en orden a la elaboración automática de los datos de carácter personal del Consejo de Europa de 1980, establece en su artículo 12, que ninguno de los países signatarios podrá, con el único fin de proteger la privacidad, prohibir o someter a autorización especial el flujo transfrontera de datos personales que se envían a otro país firmante. Sin embargo la misma establece dos excepciones, a saber:

1. Se incluye el principio de reciprocidad o de equivalencias, como lo llama la Convención, en virtud del cual se puede prohibir la exportación de aquellos datos con respecto a los cuales no exista una protección equivalente en el país importador.

2. Se evitan ventajas o incentivos, en favor de los llamados paraísos informáticos (países sin controles ni obligaciones sobre los datos sensibles y no sensibles), por lo que no se pueden transferir informaciones a otros países no signatarios que se sustraigan de las obligaciones dimanantes de la Convención.

B. Transferencias Electrónicas de Fondos a nivel internacional.

Se reconoce la existencia de una transferencia internacional de fondos, cuando el transmitente de una transferencia da al banco la orden de transferir fondos al adquirente en un banco ubicado en el extranjero. En estos casos, la transferencia de fondos entre adquirente y transmitente es internacional, no obstante operaciones tales como: la orden del transmitente de proceder a la transferencia, el débito en la cuenta por el banco del transmitente y el crédito en la cuenta del adquirente se considerarán

operaciones nacionales como si se tratara de una transferencia local de fondos. Se dice entonces que para que haya una transferencia internacional, debe haber una o más operaciones de transferencia de fondos entre bancos de países distintos, o una o más operaciones de transferencia de fondos en el país del transmitente y en el país del adquirente.

Actualmente no existen normas aplicables a las transferencias internacionales, salvo aquellas que rigen para ciertas redes como la SWIFT y aquellas que rigen las transferencias mediante tarjetas de crédito o débito realizadas mediante ciertas compañías transnacionales (VISA, MASTERCARD, DINERS CLUB, AMERICAN EXPRESS, CIRRUS, PLUS, etc.). Lo cierto es que ante tales operaciones, las normas de conflicto consideraran como competentes para conocer de un conflicto determinado a la legislación de uno de los países involucrados. Ello implica que tal legislación deberá tomar en cuenta que una parte de la transferencia se tramitó en un país extranjero de conformidad con las leyes y las prácticas bancarias del mismo.

Hay un sector de la doctrina que se inclina por aplicar a las transferencia internacionales de fondos, del proyecto de Convención sobre letras de cambio internacionales y pagarés internacionales de la UNCITRAL (Comisión de las Naciones Unidas para el derecho mercantil internacional), el cual declara ser aplicable a las transferencias bancarias de fondos. No obstante esta Convención sólo resultará aplicable si las partes así lo declaran, tal y como lo señala la misma.

C. Ley aplicable.

En el caso de la determinación de la responsabilidad civil contractual, el criterio imperante en el derecho internacional Privado, resulta ser la aplicación de la ley del lugar en el cual los contratos se realizan o ejecutan, es decir el sitio de cumplimiento de las obligaciones. Este sitio puede inferirse de la voluntad expresa de las partes. Pero si las partes no han determinado el lugar de cumplimiento, hay que buscar su voluntad tácita, que puede surgir de circunstancias accidentales, como el pago, trabajos, ejecutarse sobre el inmueble, etc. Y como último recurso habrá de presumirse que el deudor cumplirá la obligación en su domicilio.

Tratándose de la responsabilidad civil extracontractual, la Doctrina se inclina por el principio de *lex loci delitii commissi*, o sea la aplicación de la ley del lugar en el cual ocurre el hecho dañoso. Esta posición resulta aceptada por la Ley 15 de 26 de setiembre de 1928, mejor conocida como Código de Bustamante, en sus artículos 167, 168, y 302.

Lo cierto es que ha falta de normas de derecho internacional Privado aplicables a la materia, se plantea la recopilación de los usos bancarios que integrando la *Lex Mercatoria*, llenen el vacío normativo sobre este particular. Ya instituciones como la UNCITRAL y la Cámara de Comercio Internacional con sede en París, adelantan reglas uniformes de aplicación internacional que en el futuro servirán de base para definir los derechos de los usuarios de los servicios bancarios internacionales a través de la

informática, la cual será fuente de derecho como uso o costumbre de carácter normativo y por las referencias que a las mismas se hagan en los contratos bancarios.

CAPÍTULO TERCERO: BIENES E INTERESES JURÍDICOS AFECTADOS Y SUPUESTOS DE RESPONSABILIDAD DEL BANCO

I. Bienes e intereses jurídicos afectados.

A. El patrimonio.

El patrimonio de un cliente que puede verse afectado por un hecho informático bancario, será el constituido por todos aquellos bienes que éste confía a la entidad bancaria o que espera recibir de ésta y que de alguna forma pueden verse afectados por el procesamiento o almacenamiento electrónico que de la información referente a éstos, efectúen las entidades bancarias. Es así que siendo la lesión o menoscabo que afecta un interés relativo a los bienes de una persona, un daño patrimonial, serán daños patrimoniales los que cause el banco a su cliente en razón del uso de sistemas informáticos para el procesamiento electrónico de las operaciones y la información que es inherente a dicho cliente, cuando tal uso lesione un interés relativo al patrimonio de éste. Este daño patrimonial puede devenir tanto en un daño emergente, es decir en una disminución actual de los activos del cliente que el banco puede afectar con sus acciones u omisiones, o en un lucro cesante, es decir, la privación de los réditos futuros que el cliente debería obtener (derecho adquirido y cierto) de los activos que por el actuar o no actuar del banco, ya no tiene y aun en la denominada "pérdida de un chance", es decir la frustración de una expectativa o probabilidad de ganancia futura (Zannoni, 1993: 74).

Los daños patrimoniales que un banco puede irrogar a sus clientes a través del uso de la informática, se platean principalmente mediante hechos relacionados con las transferencias electrónicas de fondos (TEF). Por tal razón profundizaremos en la

regulación de estas operaciones en una de las legislaciones más completas sobre este particular, la legislación de los Estados Unidos de América.

1. La responsabilidad patrimonial por las transferencias electrónicas de fondos: la legislación de los Estados Unidos de América.

La prevención o indemnización de los daños causados por las TEF, han sido la causa de legislaciones especiales en distintos países. Una de las más completas es la de los Estados Unidos de América, en donde se aprobó la *Electronic Fund Transfer Act* (*EFTA*) de 10 de noviembre de 1978, que forma parte de la *Consumer Credit Protection Act*. Esta legislación sufrió algunas reformas con la *New Uniform Payments Code* (*NPC*).

La relevancia de la mencionada información radica en que de forma indirecta la misma ha influido en los reglamentos que en nuestro país, los bancos han adoptado para regular sus operaciones de TEF. Ello en razón de que en muchos casos, siendo el de las TEF uno de ellos, los principios y lineamientos generales consagrados en la reglamentación de los bancos de los Estados Unidos de América con sucursales en Panamá, han sido acogidos en las reglamentaciones del resto de los bancos de la plaza panameña, sean estos privados o estatales. Tal situación es en gran parte el resultado de la falta de una legislación propia sobre estas operaciones. Es así que consideramos pertinente efectuar algunos comentarios sobre el régimen jurídico y los problemas que ocasionan las TEF, en el marco de la *EFTA*.

La *EFTA* prevé la responsabilidad civil de los bancos por el incumplimiento de las órdenes de transferencia y por la realización de transferencias no autorizadas.

Tratándose de las TEF, en virtud del contrato que les da nacimiento a las mismas, el banco se obliga, conforme a la *EFTA*, a pagar o realizar un pago (aun en efectivo) a favor de un beneficiario, o del banco del beneficiario, en razón de una instrucción del contratante. En estos casos el banco actúa como mandatario de su cliente.

Por otra parte se establece que el banco ha cumplido la orden cuando: transmite la orden de pago, comunica al beneficiario que la orden fue transmitida o comunica al banco del beneficiario que la orden será transmitida. Y lo anterior siempre y cuando el banco del pagador no revoque la orden.

A pesar de lo anterior, no existe un consenso en cuanto al momento en el que una transferencia de fondos puede considerarse como definitiva y por lo tanto iniciarse sus efectos legales. Inclusive se señala que la transferencia puede adquirir el carácter definitivo, en momentos diferentes con relación al banco o bancos que las realizan, al transmitente o al adquirente de la misma.

Algunos actos pueden dar carácter definitivo a la transferencia, entre ellos tenemos: el débito en la cuenta del transmitente, la acreditación de la cuenta del banco del adquirente, el aviso de la acreditación de la cuenta del banco del adquirente, la decisión del banco del adquirente de aceptar la transferencia de crédito, el asiento de crédito en la cuenta del adquirente, el hecho de que el mencionado asiento de crédito se haga irreversible, cuando el adquirente ha recibido el aviso de crédito correspondiente, cuando el banco del adquirente entrega la suma de dinero en efectivo al adquirente. Todo dependerá del sistema jurídico de que se trate y de la legislación interna de cada país.

En lo que respecta a la transferencia de débito, habida cuenta que son definitivas desde la ejecución de los actos pertinentes por parte del banco del transmitente, éstas se sujetan a las mismas posibilidades a las cuales nos hemos referido, tratándose de las transferencias de crédito, para los efectos de determinar su carácter definitivo.

Únicamente existe una posible excepción y es el caso de la acreditación de la cuenta del adquirente, ya que la misma no perfecciona la transferencia de débito, pues tal acreditación resulta cancelable si la orden de transferencia de débito no es atendida, como puede ocurrir con el depósito de un cheque.

Tratándose por su parte, de las transferencias de fondos interbancarias, incluyendo aquellas que se producen por medio de la telemática (de computadora a computadora), el asunto se torna aún más complejo, pues puede ocurrir que en el proceso intervengan múltiples bancos. Lo cierto es que la transferencia no se tendrá por perfeccionada sino hasta que se surta todo el trámite establecido en los acuerdos interbancarios o en las normas pertinentes.

En otro sentido, la introducción de los procesos informáticos ha determinado que las órdenes de transferencias de fondos no sean atendidas inmediatamente, como ocurre en el procesamiento por lotes (*batch*), así es que las mismas pueden ejecutarse anticipadamente al día en el que deberían hacerse efectivas o aunque su atención sea ejecutada al día siguiente de entregada la orden. Tratándose de procesamiento de datos en línea (*on line*), en el cual los asientos de débitos y créditos se realizan directamente en las cuentas pertinentes, los bancos asientan tales débitos y créditos en cuentas provisionales, las cuales luego se refunden con las cuentas ordinarias, luego de la liquidación interbancaria o cuando el banco lo considere apropiado. En este caso la computadora puede mostrar los balances de las cuentas provisionales. De esta forma las transferencias no tendrán el carácter de definitivo hasta que las cuentas provisionales se fusionen con las ordinarias. Si se tratara de terminales *off line* o fuera de línea, activadas por el cliente, las mismas almacenan los datos en sus memorias para luego ser procesados por lotes, aplicándose en lo posible las reglas de las transferencias por lotes. Si la transferencia es *on line*, como ocurre con mayor frecuencia, tratándose del uso de cajeros automáticos (*ATM'S*), el carácter definitivo de la transferencia puede

considerarse desde el momento en el que el cliente recibe el dinero, y el asiento de débito en la cuenta del cliente sería tan sólo un trámite tendiente ha dejar constancia de la ocurrencia de la operación.

Ahora bien, el incumplimiento de la TEF, va a implicar, como resulta lógico suponer, el surgimiento de una responsabilidad contractual para el banco, tanto por el hecho de una acreditación errónea de una suma indebida a la cuenta de un cliente, como en el caso de incumplimiento de una orden autorizada.

Según la legislación analizada, un incumplimiento de una orden de transferencia electrónica de fondos es injustificado cuando: "el banco del contratante omite pagar o transmitir la orden de pago al otro banco durante el mismo día hábil en el cual se ha recibido la orden" (Giannantonio, 1989b: 27). La responsabilidad que surge para el banco en estos casos, se extiende a lo que esta legislación denomina: ***all actual damages proximately caused***, o sea todos los daños directos e inmediatos causados al contratante por el incumplimiento injustificado de órdenes autorizadas y los ***consequential damages***, o sea los daños indirectos ante un incumplimiento doloso. En este último caso, también se han establecido diferencias, si el incumplimiento es el resultado del actuar del banco pagador, del transmisor o del banco que recibe la suma de dinero. Si el responsable fuese el banco pagador, la responsabilidad por daños indirectos subsiste sólo cuando hay dolo; en el caso de ser responsable el banco que recibe los fondos, subsiste aún por errores de elaboración o errores no intencionales.

No subsistirá la responsabilidad del banco, si el incumplimiento de la orden se produce por falta de fondos en la cuenta del cliente, o cuando dichos fondos estuvieren embargados o sujetos a otras medidas cautelares y también cuando la transferencia excediese los límites del crédito.

No obstante lo anterior, el banco se exonera de responsabilidad, si el mismo comprueba que el incumplimiento fue ocasionado por: 1) caso fortuito o fuerza mayor;

2) por defectos técnicos conocidos por el cliente al momento de emitirse la orden de transferencia o tratándose de transferencias preautorizadas, al momento en que la transferencia debió producirse. Cabe advertir que por transferencias preautorizadas debe entenderse aquellas autorizadas de antemano y a efectuarse nuevamente a intervalos fehacientemente regulares (Giannantonio, 1989b: 100).

Si un defecto en el sistema informático impide que se efectúe una TEF y el beneficiario de la misma hubiese aceptado el pago por vía electrónica, la obligación del emisor de la orden en favor del beneficiario de la misma resultará suspendida hasta que se corrija el desperfecto y la transferencia se efectúe, salvo que se requiera el pago por otros medios.

La legislación en comento, elimina la necesidad de verificar que el banco tiene conocimiento de las consecuencias dañosas que ocasionan un incumplimiento y el grado de diligencia adoptado, consiguiendo una mayor seguridad jurídica y evitando largos litigios.

Resulta relevante el hecho de que el banco receptor generalmente no esta al tanto del negocio subyacente a la transferencia y por lo tanto le es difícil establecer el impacto de su negligencia al proceder con la acreditación de los fondos. Además, si éste incurre en una incorrección al cumplir con la orden de transferencia, la misma es por lo común justificable.

Los errores en las transmisiones de mensajes electrónicos se producen sobre todo en las transferencias electrónicas internacionales, a través de megaredes y en razón de malas traducciones de los mensajes

Por otra parte, una transferencia electrónica de fondos se considera no autorizada, cuando la misma es efectuada de la cuenta de un cliente por una persona carente de un poder o autorización legal y el cliente no recibe ningún beneficio con la operación. Sin embargo, no se considera la transferencia como comprendida bajo el

concepto de no autorizada, si la misma es efectuada por persona distinta del tarjetahabiente o cliente que tenga en su poder la tarjeta, el código u otro medio de acceso, a menos que el cliente haya notificado al banco que las transferencias efectuadas por terceros debían considerarse como no autorizadas, así como también los casos de transferencias electrónicas efectuadas de forma fraudulenta por el propio cliente o terceros en combinación con éste y finalmente los casos de errores del banco. En estos casos, los daños o bien son asumidos por el cliente, o bien son asumidos por el banco. Sin embargo, conforme a la primera opción, la magnitud del riesgo sería gravísima para el cliente y en el caso de la segunda, el aumento provocado en los costos los asumiría en definitiva el cliente, el cual descartaría el uso de estos mecanismos. Por ello se propone una respuesta equitativa que parte de una responsabilidad fundada en la culpa y el establecimiento de una limitación del resarcimiento. Es así que será responsable quien incurra en culpa, siendo el resarcimiento al que estaría obligado equivalente a los daños directos e inmediatos.

Para algunas reglamentaciones, la culpa del cliente se reduce a: 1) el escribir su número de identificación personal en la tarjeta, 2) llevar la tarjeta junto con el número de identificación personal, 3) el dar la tarjeta y el código a un tercero que efectuó la operación no autorizada y 4) el no advertir al banco de una transferencia no autorizada dentro de un término razonable fijado por el banco, luego de recibir el estado de cuenta o de efectuada la transacción no autorizada o el no efectuar la advertencia en la forma establecida por el banco. En este último caso, vale advertir que el aviso de pérdida será generalmente oponible al banco sólo luego de transcurrido un período razonable de tiempo para que el banco proceda al bloqueo de la cuenta. Lo cierto es que en términos generales pareciera que el banco sólo resultará responsable luego de que se le haya dado aviso de la pérdida de la tarjeta y éste tuviese tiempo de adoptar las medidas para inutilizar su uso o el del número de identificación personal.

No obstante lo anterior, de forma subsecuente se advierte la responsabilidad del banco por la omisión en efectuar la transferencia previa instrucción del cliente, exceptuando los casos en los que los fondos en la cuenta del cliente no resulten suficientes, los mismos se encuentren judicialmente retenidos, la orden excediese el límite de crédito de la cuenta o la terminal no tenga suficiente dinero en efectivo. El banco también será responsable si la insuficiencia de fondos en la cuenta del cliente se debe a una falta del banco en efectuar un depósito en la cuenta del cliente o cuando el banco no detenga a tiempo el pago de una transferencia preautorizada habiendo sido previamente instruido en tal sentido.

A pesar de lo anterior, todavía hay quienes objetan la preponderancia de la teoría de la culpa por considerar que promueve largos y tediosos litigios en estos casos. Por ello, la Legislación norteamericana en referencia, prefiere combinar como ya dijimos, los conceptos de responsabilidad culposa y del límite de responsabilidad. Así se establece una responsabilidad para el cliente hasta de cincuenta dólares por transferencias no autorizadas y hasta de quinientos dólares cuando el cliente ha omitido avisar al banco la pérdida o robo de la tarjeta magnética dentro de los dos días del conocimiento del extravío o robo. La responsabilidad será ilimitada en el caso de que el cliente no avisare al banco sobre las transferencias no autorizadas o los errores en la cuenta reflejados en el estado de cuenta que le hubiese enviado el banco, en un plazo de sesenta días posteriores a la fecha del estado de cuenta. Sin embargo, aún este sistema objetivo, carente de culpa, ha sido criticado por que se dice que hace recaer la carga de la reparación sobre los clientes y bancos más diligentes quienes deben soportar los costos económicos de la medida. Esto es así por cuanto va a resultar lógico que los bancos limiten el uso de las transferencias para operaciones de menor cuantía.

En todo caso, la carga de la prueba de la culpa del cliente le compete al banco.

En otro aspecto, conviene tener presente en el caso de las TEF, que por un lado tenemos las obligaciones derivadas de la transferencia y por el otro las obligaciones derivadas del negocio subyacente, que por lo común no involucra a las mismas personas, pues por una lado esta la relación entre los bancos y sus clientes, entre los bancos y entre los clientes. En el caso de la legislación en referencia, ésto se deja claramente establecido.

Tratándose de las tarjetas de crédito y los puntos de venta (POS), éstos son programados para que se acredite al adquirente o al comerciante beneficiario, la cuantía de la orden de transferencia de débito, aun cuando la orden resultare falsa. Esto es lo que se conoce como una transferencia garantizada. De esta garantía se derivan algunas consecuencias prácticas, tales como el hecho de que el banco del transmitente esta obligado de forma irrevocable ante el adquirente y su banco a ejecutar la orden de transferencia de débito a su presentación. Así también, el banco del transmitente no tendrá derecho a retirar la orden de transferencia de débito, pues su obligación será irrevocable. Pero esta garantía de pago también implica que en caso de secuestro o embargo, tales acciones no podrían afectar la cuantía de la transferencia, en el caso de que aún la cuenta del transmitente no hubiese sido debitada.

En el caso de las tarjetas con microcircuito, también llamadas tarjetas inteligentes, las normas sobre el carácter definitivo de las transferencias parecieran ser las mismas que hemos mencionado para los casos de las transferencias garantizadas. Estas tarjetas inteligentes se caracterizan por ser susceptibles a ser cargadas por el banco del transmitente con un valor específico (un límite de disponibilidad de fondos), debitando en el acto la cuenta del transmitente. Cuando se compran bienes o servicios con la tarjeta, el calor disponible en la tarjeta es reducido por los terminales de los puntos de venta de los comerciantes. En este momento el banco del adquirente acredita la cantidad de la compra en la cuenta del adquirente en línea o en su defecto, fuera de

línea. Así el carácter definitivo de la transferencia se producirá al momento de la compra de los bienes y los servicios o después, mientras que el débito, como ya dijimos se producirá de hecho, al momento de cargarse la cuenta.

También se producirán conflictos en materia de TEF, en relación con algunas situaciones particulares como las siguientes:

1. En el caso de terceros demandantes del transmitente, aunque no parece que los mismos puedan tener derechos sobre la cuantía de una transferencia ya efectuada, toda vez que en estos casos, ya existe un valor cuya propiedad a sido transferida a otra persona, o sea el adquirente. A menos, a nuestro juicio, que la transferencia haya tenido la intención de defraudar a los acreedores del transmitente, en cuyo caso el tercero acreedor podría recurrir a acciones penales y/o civiles contra el transmitente, y en el caso de una acción pauliana, tratar de anular la operación de transferencia.

2. Cuando el transmitente fallece y el banco conoce del fallecimiento antes de efectuar la transferencia, el mismo no deberá realizar la misma o de lo contrario podría incurrir en responsabilidad. Sin embargo, en ciertos casos (art. 1409 del Código Civil), se faculta al mandatario, en este caso el banco, a seguir adelante con la ejecución del mandato, o sea de la transferencia, para no perjudicar los intereses del cliente, es decir del transmitente, aun luego de conocida su muerte. No obstante ello, algunas legislaciones determinan que el banco no ejecute la transferencia en estos casos cuando reciba una instrucción en contrario, de quien tenga un interés legítimo sobre los fondos, tales como herederos comprobados.

3. En el caso de que se inicie un proceso de concurso de acreedores o de quiebra del transmitente, el banco se verá también impedido de atender las ordenes de transferencias no definitivas. En algunos países la prohibición de atender las

órdenes de transferencia, en estos casos, se produce inclusive aunque el banco no tenga conocimiento oficial del inicio del concurso de acreedores o de quiebra.

4. Tratándose de la incapacidad legal del transmitente por minoría de edad, demencia u otras causas, la revocación de las transferencias efectuadas, aún de las definitivas, pareciera un hecho inevitable.

5. En caso de embargo de la cuenta del transmitente, si se hubiese efectuado una transferencia que aún no fuese definitiva, y el embargo fuese conocido por el banco, según la doctrina, la medida judicial podría afectar la cuantía en proceso de ser transferida. Sin embargo, en el caso de una transferencia de crédito, algunas legislaciones consideran que si ya se hubiese debitado la cuenta del transmitente, la medida judicial no afectaría la cuantía en proceso de transferencia, pero otras consideran que si la transferencia aún no fuese definitiva, sí se afectaría. Algo más complejo resultaría el evaluar la responsabilidad del banco transmitente en el caso de que la transferencia se efectuase a través de bancos intermediarios, ya que si un embargo afectase la transferencia efectuada, pero que no ha adquirido el carácter definitivo, el banco del transmitente debería efectuar esfuerzos razonables por evitar el perfeccionamiento de ésta o demostrar que los ha hecho, para el caso de que la misma se perfeccione al final.

6. Sucede también que si la transferencia no es irrevocable, el cliente puede retirar la orden de transferencia si ésta no ha adquirido el carácter de definitiva. En estos casos el banco del transmitente deberá adoptar las medidas para que la transferencia no se perfeccione, aún frente al banco del adquirente.

Cabe advertir que el banco no resultará obligado, salvo por las excepciones planteadas, a detener el trámite de una transferencia, si el mismo no ha sido notificado de alguna situación que implique una obligación, de evitar el perfeccionamiento de la transferencia. Así también, se establece en algunas legislaciones que no sólo bastará el

aviso, sino también que luego de dado éste, el banco deberá contar con un término razonable para adoptar las medidas que se deriven de haberlo recibido.

Otro aspecto importante es el de las llamadas transferencias de fondos por error del banco. La *Electronic Transfer Fund Act*, sección 908 define tales errores como: "una transferencia electrónica de fondos no autorizada o, el recibo de una cantidad incorrecta de dinero obtenida de una terminal electrónica, por el consumidor" En estos casos el problema se produce porque hay que determinar si el banco puede corregir el error o si no puede hacerlo, por el carácter definitivo de la transferencia. Sin embargo, los bancos para disminuir los riesgos que ésto implica, asientan los débitos y los créditos con carácter provisional hasta que se haya verificado la autenticidad de las órdenes, la exactitud del procedimiento de los datos y la garantía de que el banco recibirá un valor del deudor. Pero si la transferencia adquiere una carácter definitivo, la cancelación de los cargos asentados será restringida. Sobre esto se presentan diversas situaciones:

1. Si el banco es conocedor de lo fraudulento de la transferencia y no obstante ello la ejecuta, el banco será responsable de las pérdidas causadas.

2. Si el banco es instruido por el transmitente del retiro de la orden de transferencia y aún así la ejecuta, el banco será responsable por el daño causado al cliente.

Ahora bien, toda vez que la obligación del banco en razón de la transferencia de crédito, resulta cumplida cuando la transferencia adquiere el carácter de definitiva, su cliente podrá reclamarle los daños sufridos por las demoras o atrasos incurridos en el cumplimiento de la orden. No sucede igual tratándose de las transferencias de débito, pues en tal caso será el adquirente de la transferencia quien soportará el riesgo con respecto al transmitente por las demoras o errores en el proceso de transferencia de fondos. En ambos casos se discute sobre la responsabilidad de la compañía de telecomunicaciones públicas. Para algunos, ésta debe asumir una responsabilidad, para

otros no. Si no lo hace la responsabilidad recaería sobre el transmitente o sobre uno de los bancos. Para unos, el transmitente debe asumir la pérdida, toda vez que la transferencia se hace para su beneficio y no existe otra persona a quien pueda imputársele la responsabilidad. Por su parte quienes alegan que la responsabilidad deba asignársele a uno de los bancos, señalan que éstos son los responsables de escoger el sistema de transferencia de fondos, inclusive mediante la utilización de los servicios públicos de telecomunicaciones, por lo cual cualquier demora o atraso puede avisárseles con tiempo suficiente para que adopten las medidas correctivas del caso. Tal responsabilidad puede recaer ya sea en el banco del transmitente, como responsable de la ejecución adecuada de la transferencia o el banco expedidor de la orden perdida, demorada o alterada.

Lo anterior no implica que no haya quienes señalen que la responsabilidad del banco en estos casos no existe, toda vez que las demoras o pérdidas de órdenes no es más que el resultado de problemas técnicos que escapan al control del banco. De hecho los bancos suelen incluir cláusulas exoneratorias de responsabilidad en estos casos. Sin embargo, la validez de tales cláusulas y en general, lo acertado del criterio de exoneración total del banco, queda desvirtuado por el hecho de que las fallas del computador pueden ser el resultado, como ya hemos señalado (Supra, págs. 115 y siguientes), de un equipo o programas inadecuados, o bien de un deficiente o inexistente mantenimiento, por lo que tales fallas pueden ser reducidas, si el banco ejecuta una adecuada planificación y cumple con las obligaciones técnicas detalladas en el capítulo anterior (Supra, pág. 111).

La *Electronic Transfer Fund Act* regula la responsabilidad de las entidades financieras por los errores en las transferencias de fondos en las secciones 909 y 910.

Si tratándose de los supuestos de hecho antes vistos, se concluyera que la responsabilidad recae sobre un empleado de la empresa de telecomunicaciones, los

servicios de comunicación de datos, la red de transferencia electrónica de fondos o la cámara de compensación electrónica, tales empresas podrían considerarse responsables, salvo que se trate de un fraude cometido en razón de los conocimientos del empleado durante el curso de su trabajo tal y como afirmamos con anterioridad (Supra, pág. 91).

Tratándose de quién debe probar la existencia del daño y su imputabilidad, existen criterios divergentes. Por un lado quienes sostiene que debe ser el cliente, lo cual determinaría que si una transferencia no fue autorizada, éste debe demostrar la responsabilidad del banco, o su reclamación o demanda resultarán ineficaces. Si es el banco quien debe demostrar que la transferencia fue autorizada, entonces podría ser que el resarcimiento del probable daño causado al cliente fuese algo más probable. Sin embargo, las pruebas que quedan, después de efectuarse una operación de transferencia de fondos, sea a través de cajeros automáticos o puntos de venta, resultan tan escasas (sólo el registro de la cuenta) o tan insuficientes para demostrar que hubo un error no detectado por la computadora o por el acceso no autorizado de un cliente a la misma (en ambos casos con la posible negligencia o complicidad del cliente) que siempre se asigna la carga de la prueba al cliente para demostrar que hubo una irregularidad que es imputable al banco y que le ha irrogado un daño. Es por ello que generalmente el banco, incluye una cláusula en sus contratos con el cliente, de tal forma que sea éste quien asuma toda la responsabilidad sobre las operaciones efectuadas con su tarjeta magnética (débito o crédito) u otros dispositivos de acceso, salvo después de avisar la pérdida o sustracción ilícita de la tarjeta u otros dispositivo de acceso a la computadora.

En el caso de pérdidas, demoras o errores de una orden de transferencia interbancaria, sin que pueda determinarse el origen del problema, pareciera lógico suponer que será uno de los bancos quien deberá sumir la carga de demostrar que no es

responsable de la pérdida. En este caso lo sería, generalmente, el banco del transmitente. Sin embargo, si este no fuese responsable por disponerlo así la legislación aplicable, entonces corresponderá al propio cliente transmitente, quien deberá probar que su banco fue el responsable, lo cual se dificultara si tal banco es extranjero.

Se señala también, que en caso de demoras o errores en la tramitación de una orden de transferencia de fondos, la indemnización del banco hacia el cliente puede surtirse fácilmente mediante el pago de intereses o una suma equivalente a las pérdidas. Pareciese que el banco conforme a la legislación civil general, no debiese asumir responsabilidad por consecuencias no previstas o no previsibles razonablemente. Sin embargo, se señala que hay casos en los cuales el banco conoce tanto el propósito de la transferencia como los efectos que resultarían de las demoras o errores de su tramite. Por ello algunos opinan que el banco debería asumir la responsabilidad por el daño emergente ocasionado por sus errores o demoras, ya sea que se trate del banco del transmitente o de los otros bancos dentro de la cadena de la operación interbancaria.

2. La responsabilidad patrimonial en las nuevas tecnologías bancarias.

En otro aspecto, tratándose de las tarjetas inteligentes y del dinero o moneda E (electrónico) que surge al propiciar la transferencia de valores monetarios por medios electrónicos, se van desarrollar problemas jurídicos que pueden afectar negativamente el patrimonio de los clientes de los bancos de forma más dramática que lo que ocurre con las transferencias electrónicas de fondos, y cuya solución siendo más difícil, implicará el aumento de los riesgos para los usuarios de los servicios que los bancos

pueden ofrecer en este sentido. Pensemos tan sólo en el hecho de que se produzca la pérdida de una tarjeta inteligente, pues tal situación va a resultar análoga o equivalente a la pérdida de dinero en efectivo y por ende la posibilidad que el tarjetahabiente tenga que afrontar la totalidad de los daños dimanantes de la pérdida de la tarjeta, en razón del uso que terceros le puedan dar a la misma, apropiándose de los valores monetarios en ella insertos. En este caso, prácticamente no habrá mayor responsabilidad que pueda endilgársele al banco. Tampoco habría responsabilidad para el banco, en los casos en los cuales el dinero E fuese guardado en el disco duro del computador del cliente y por una caída del sistema o un error del propio cliente en el accionar de su computador, los registros del dinero se borraran. Desde que el dinero E es transmitido de la memoria del computador del banco a la tarjeta inteligente o a la memoria del computador del cliente, la pérdida o inclusive la sustracción de dicha información, no implicará, en ningún caso, responsabilidad para el banco, eximiéndose este en razón del actuar de terceros o del propio cliente como víctima.

Quienes recurran a estas novísimas herramientas tecnológicas, deberán asumir, a falta de Ley que diga lo contrario, los riesgos que las mismas conllevan, pues pudiendo optar por medios más tradicionales y menos riesgosos, han optado por lo que les ofrece la tecnología llamada de punta, en lo que les beneficia y en lo que les puede perjudicar.

B. La intimidad

1. Concepto y alcance.

Los derechos de la personalidad pueden definirse como aquellos derechos subjetivos cuyo objeto son los bienes jurídicos atribuidos al ser humano en su condición de persona. Se diferencian de los derechos humanos sobre la base de que estos surgen en virtud de la función que las personas cumplen dentro de la sociedad en la cual se desenvuelven, mientras que los derechos de la personalidad surgen en virtud de la propia existencia de la persona con prescindencia de su vinculación o no a una sociedad determinada. Son aquellos que guardan mayor relación, ya no con el elemento función sino con el elemento libertad.

Constituyen derechos de la personalidad: el derecho a la propia imagen, el derecho a la intimidad, el derecho al honor, el derecho a la identidad y también el derecho a la propia libertad de actuar.

En el caso específico de la intimidad, ésta ha sido definida por Meján, en función exclusiva de las personas naturales o físicas, así:

> .....el conjunto de circunstancias, cosas, experiencias, sentimientos y conductas que un ser humano desea mantener reservado para sí mismo, con libertad de decidir a quién le da acceso al mismo, según la finalidad que persiga, que impone a todos los demás la obligación de respetar y que sólo puede ser obligado a revelar en casos justificados cuando la finalidad perseguida por la develación sea lícita (Meján, 1994: 87).

Por su parte el derecho a la intimidad, ha sido definido sin distinguir la naturaleza de la persona, por el mismo autor, como:

> El Derecho a la Intimidad o Privacia es un Derecho Fundamental que asiste a los sujetos de derecho consistente en la facultad de mantener reserva sobre diversas situaciones relacionadas con la vida privada, que debe ser reconocido y regulado por el sistema jurídico y que es oponible a todos los demás salvo en los casos en que

> puede ser develado por existir un derecho superior de terceros o para el bienestar común (Ibidem: 105).

El contenido de este derecho esta constituido en principio, por las situaciones de la vida privada de una persona que ésta desea mantener en reserva, las cuales pasan a constituir información que es recogida, conservada, clasificada y utilizada para un fin determinado y autorizado previamente por aquél al cual la misma concierne y no con otros objetivos. Decimos en principio, porque según veremos (Infra, pág. 151), la evolución legislativa a llevado a las normativas más modernas a considerar el derecho a la intimidad como un derecho de control sobre la información que concierne a las personas. En cuanto a los sujetos de este derecho, hay un sujeto activo, o sea aquella persona que resulta titular del derecho; también hay un sujeto pasivo, es decir, todo aquel con posibilidades de entrometerse o afectar negativamente el derecho a la intimidad de una persona y que por lo tanto tiene el deber de respetar tal derecho o en caso contrario causar un daño.

Se menciona la existencia de cuatro elementos fundamentales de la noción de intimidad, a saber: el secreto o reserva, el derecho de control de la utilización y circulación de la información confiada por una persona a un tercero y la tranquilidad o ausencia de perturbación física o psicológica y la autonomía.

La intimidad como bien jurídico resulta tutelado tanto en el ámbito de la protección civil, como en el ámbito de la protección administrativa y en el ámbito de la protección penal.

Para algunos, con un concepto restrictivo por cierto (sólo hacen alusión a los datos nominativos), esta protección de la intimidad puede reflejarse en la siguiente equivalencia conceptual:

Intimidad = datos nominativos = información personal automatizada (Jijena Leiva, 1992: 36).

Un sector importante de la doctrina distingue entre el concepto intimidad, que determina como aquel sector del hombre perteneciente a su ámbito interno, al que no tiene acceso el mundo y sobre el que puede disponer sin ser molestado, y la esfera privada o vida privada, concepto más amplio que el anterior, que aludiría a aquel sector vital que se manifiesta y trasciende al mundo de las conductas, pudiendo ser accesible a cualquier persona. En este caso la vida privada sería el género y su especie principal: la intimidad (Jijena Leiva, 1992: 37). Y es que hay informaciones personales que distinguen a una persona dentro de una sociedad y que la Doctrina considera como de propiedad pública y de uso común o como los denomina Frosini (Frosini, 1988: 76): datos personales esenciales (entre ellos: el nombre, el domicilio, el número de teléfono, la profesión, lugar de trabajo, estado civil y otros), mientras que otros no vinculados con la sociedad y por lo tanto de carácter privado, sólo deben ser utilizados por entidades específicas y para fines específicos (entre ellos: el estado de salud, el patrimonio, las deudas, la religión, las ideas políticas etc.). Estos últimos son los datos sensibles, los cuales constituyen el ámbito íntimo y por lo tanto tutelado por la ley. Parellada los define como: ".....los referidos a circunstancias de orden personal que la persona desea que no trasciendan fuera de su esfera íntima o que pueden ser utilizados en forma discriminatoria" (Parellada, 1990: 361). No obstante ello, resulta preciso advertir que en relación con los datos o información tutelada, la tendencia moderna, como se refleja entre otras, en la jurisprudencia alemana (Denninger, 1987: 273), es que no sea la clasificación abstracta o categórica de una información según su cercanía al concepto intimidad, ni que por su naturaleza sea considerado secreto o no, lo determinante para considerarlo como sensible, sino más bien su utilidad y la posibilidad de su aplicación.

La evolución del concepto jurídico intimidad, ha partido de la concepción individualista de Warren y Branderis en 1890 [3] ,la cual hizo equivalente el mismo a un derecho al aislamiento, para concebirse hoy en día como el derecho a controlar la información que sobre las personas es objeto de tratamiento por parte de diversos organismos públicos y privados, entre ellos las entidades bancarias. Es decir, se ha pasado de lo que puede denominarse una libertad negativa a una libertad positiva, o sea de una libertad de rechazar la divulgación de información sobre sí mismo, a una libertad de controlar el uso de la información que de sí mismo tienen otras personas(Jijena, 1992: 47). El precedente más importante, en este sentido, lo encontramos en la doctrina alemana sobre autodeterminación informativa contenida en sentencia del Tribunal Constitucional Alemán, en razón del establecimiento del número de identificación nacional. El órgano constitucional en este caso sentenció que para recopilar datos sobre un determinado ciudadano se requería su consentimiento previo.

2. Intimidad e Informática bancaria.

La intimidad es un derecho de la personalidad y el interés de la persona que es titular del mismo, es susceptible de ser lesionado o menoscabado por el hecho informático bancario, puesto que la esencia de tal hecho informático consiste en

---

3 Samuel D. Warren y Louis D Branderis fueron los creadores del moderno concepto del "right to privacy" o derecho a la intimidad El abogado Warren, luego de contraer matrimonio con la hija de un senador, inicia una vida extravagante y lujosa, de la cual se hacen eco los medios informativos del momento y el consiguiente escándalo. Warren entonces de asocia con su antiguo compañero de la Universidad de Harvard, Louis Branderis -más tarde Magistrado de la Suprema Corte de los Estados Unidos- para escribir el ensayo intitulado "The right to privacy", el cual es publicado en la Harvard Law Review. Para los autores toda persona tiene el derecho a la privacidad o intimidad conforme a la fórmula "right to be let alone", o sea a ser dejado en paz, a que se respete su soledad, su vida íntima, así como su vida privada

procesar información para ser almacenada, asociada con otra información y utilizada en interés del banco, teniendo presente que en todo caso dicha información cae dentro del ámbito de la intimidad inherente a tales personas. En tal sentido se ha llegado ha establecer la existencia de un derecho a la intimidad informática (Meján, 1994: 100), el cual tiene por objeto material, la información que sobre el cliente y su patrimonio mantiene el banco en la memoria de sus computadores.

Ahora bien, la lesión que se ocasiona al derecho a la intimidad de los clientes de un banco, debe definirse como moral, en la medida en que tal lesión, como en principio pareciera inferirse, afecte solamente intereses de naturaleza extrapatrimonial, sin embargo si produciéndose la lesión al derecho a la intimidad como bien jurídico protegido, deviniesen además daños de carácter patrimonial, es decir la afectación negativa del patrimonio actual y aun futuro del cliente, podríamos estar igualmente frente a un daño patrimonial indirecto. Y es que el perfil financiero que los bancos elaboran sobre sus clientes, es el resultado de la información contenida en sus bancos de datos, los cuales siendo inexactos o incorrectos van a afectar indeleblemente los derechos de crédito y aun el crecimiento económico de los clientes de los bancos.

En razón de lo anterior, y en virtud que de una forma o de otra la informática atomiza el dominio que tienen las personas sobre aquellas informaciones que le son propias y que la facultad que tiene los bancos de guardar, usar y difundir bajo ciertos supuestos la información intima de sus clientes, fuera de su control, puede implicar la deformación de la personalidad de éstos, difundiendo una imagen inexacta, desde una errónea construcción de los datos, es por lo que a todo individuo y muy especialmente a los clientes bancarios debe reconocérseles como mínimo, los derechos siguientes:

(a) Que no se recabe información sobre su persona sin su autorización. Para estos efectos y para todos los derechos que detallamos a continuación, toda persona debe conocer sobre la existencia de bancos de datos personales y a que los administradores de

tales bancos de datos les brinden a requerimiento, toda la información que les concierna.

(b) Sin embargo, si tal autorización se concede, la información así recabada debe ser utilizada para los fines previstos y convenidos.

(c) Igualmente toda persona debe tener derecho a solicitar la corrección de dicha información cuando la misma resulte inexacta o desactualizada. Y es que: "Con el avance de la informática no sólo es más difícil controlar la difusión de datos personales, sino también asegurar la exactitud de aquellos que se almacenan o se transmiten para diversos fines" (Correa, 1987: 241). Para estos fines las legislaciones más modernas han incluido el principio del *hábeas data*, que no es más que el derecho que tiene todo individuo a los datos que sobre su persona resultan almacenados en cualquier banco de datos y en adición, el derecho a requerir su rectificación o eliminación para el caso que los mismos hayan sido obtenidos por medios ilegales o que sean inexactos u obsoletos.

(d) También se debe reconocer el derecho de toda persona a que la información que le concierne y que sea almacenada en bancos de datos, sobre todo si resulta negativa para sus intereses, sólo sea conservada durante el tiempo necesario en función de los fines para los cuales la misma fue recogida, en lo que algunos tratadistas han denominado el derecho al perdón o también como el derecho al olvido. Este principio, vale advertir, previene del riesgo a que conduce el almacenamiento de datos en la memoria del computador, pues la misma tiene la capacidad de conservar indefinidamente los datos en sus soportes (discos duros, disquetes o *cd's*), con lo cual, si tales datos afectan negativamente el perfil personal o financiero de una persona, se atenta contra el referido derecho al perdón o derecho al olvido.

(e) El derecho a que se prohiba, salvo excepciones específicas, la conservación de información sobre aspectos raciales, políticos, religiosos, sobre el historial delictivo y otros datos denominados sensibles, toda vez que los mismos se consideran datos no

procesables. Entre estas excepciones, cabe advertir que la incorporación de estos datos a un ordenador individual no es ilícita, si la misma no es el resultado de una intromisión, como en el caso de que sea el propio cliente el que proporcione la misma, por ejemplo a un banco con el cual realiza una negociación o a la cual hace una solicitud de crédito o para la apertura de un depósito. Sin embargo, dicha información no debe rebasar el ámbito del profesional -el banquero- que utiliza dicha información para materializar un acto propio de su gestión.

(f) Y en definitiva, toda persona debe tener derecho a exigir la reparación de los daños morales o materiales que se causen por la violación de los anteriores derechos.

Estos derechos y los principios en los cuales se fundamentan, a los cuales volveremos a aludir más adelante (Infra, pág. 162), conforman lo que se denomina el *hábeas data*.

No cabe duda que el cliente del banco es titular legítimo de esta información tanto en su aspecto personal como patrimonial, pues goza del denominado derecho sobre la información, el cual en no pocas ocasiones entra en colisión con el derecho a la información, es decir el derecho a dar a conocer al público aquellos hechos, noticias o acontecimientos que son de interés general. Sin embargo, este derecho a la información que no es otra cosa que el derecho de "recolectar los datos vacantes (o públicos) para crear libremente el bien-información" (Correa, 1987: 289), no puede tener por objeto material una información que forme parte de esta intimidad de la persona, es decir una información privada, sin embargo si tal información se hiciese pública con el consentimiento de su titular o por otra causa, ese derecho a la información debe facultar a cualquiera para acceder en forma libre e igualitaria a la misma. Lo cierto es que debe existir un equilibrio entre el derecho sobre la información y el derecho a la información, pues el mismo aunque difícil, como señala Jijena (Jijena, 1992: 44), resulta

imprescindible, ya que estamos frente a derechos excluyentes pero necesarios por un lado para la sociedad y por el otro para la salvaguarda de la paz personal.

Ahora bien, cuando los datos o informaciones sobre la vida privada sean de interés público, veraces y no causen daños a la comunidad, habrá una conflicto entre los aludidos derechos, por lo cual en no pocas ocasiones habrá que limitar el derecho sobre la información que garantiza el bien jurídico intimidad, en función del interés social que representa el derecho a la información. El interés social cede entonces al interés público.

En otro aspecto, la actividad bancaria se caracteriza por recabar información de forma masiva, de tal forma que cuando esa información es tratada electrónicamente a través del uso de la informática, se presentan diversas situaciones. Una de ellas es la posibilidad de categorizar a las personas que requieren de sus servicios y que son sujetos de su información, como buenos o malos clientes. En este caso no existen reglas claras que determinen cuándo un individuo pasará de una categoría a otra, qué se requiere para cambiar de categoría o cuánto tiempo puede una persona estar en una categoría específica. Otra de las situaciones es la posibilidad de relacionar datos que aisladamente pareciesen inofensivos pero que unidos pueden conformar un perfil negativo o positivo de una persona.

Las situaciones mencionadas, es decir la categorización o interrelación de la información personal constituyen verdaderos riesgos que conspiran en contra de la intimidad, toda vez que la divulgación de la misma podría determinar una sería lesión al interés que para una persona tal bien jurídico representa. Además, el uso de dicha información personal para su aplicación en la denominada informática decisional (la toma de decisiones a través de un computador) puede ser la diferencia entre tener acceso o no a un determinado servicio u operación bancaria, con lo cual una vez más, el menoscabo de la intimidad podría implicar inclusive una afectación patrimonial

negativa por la pérdida de una oportunidad económica o también conocida como pérdida de un chance.

Para Peña Castrillón (Jijena, 1992: 41), la actividad informática de los bancos debe realizarse en el marco de una serie específica de pautas o principios, algunos de los cuales ya mencionamos y otros que detallamos ampliamente en el presente estudio, y es que como señala el mencionado autor, la informática bancaria puede ser un instrumento con capacidad para vulnerar los derechos de las personas y muy específicamente el derecho a la intimidad, por lo que los bancos deben considerar el secreto de la información procesada no sólo como un deber profesional, sino como una carga representada por el cuidado que le impone la protección de este derecho.

3. Regulación jurídica de la intimidad y la informática.

(a) Evolución de la Legislación.

Sin entrar a hacer un recuento histórico exhaustivo de lo que ha significado la protección del derecho a la intimidad, podemos establecer que ya desde la Declaración de los Derechos del Hombre y del Ciudadano producto de la Revolución Francesa de 1789, se anticipaba la existencia del derecho de todo ser humano a ser respetado en sus manifestaciones personales. Sin embargo, es a partir del artículo de Samuel Warren y Louis D. Branderis publicado en la *Harvard Law Review* en 1890, cuando este derecho empieza a ser considerado tanto a nivel doctrinal como jurisprudencial y finalmente a ser incluido en diversos cuerpos legales.

La Declaración Universal de los Derechos Humanos de la Organización de las Naciones Unidas (O.N.U.) de 1948, en su artículo 12 señala:

> Nadie será objeto de injerencia arbitraria en su vida privada, su familia, su domicilio o su correspondencia ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Tal garantía fundamental resulta consagrada subsecuentemente en el Convenio Europeo para la protección de los Derechos Humanos y de las Libertades Fundamentales de 1950, en el Pacto Internacional de Derecho Civiles y Políticos de la O.N.U de 1966, la Convención Americana sobre Derechos Humanos de 22 de noviembre de 1966. Especial significación tiene el Convenio para la Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal del Consejo de Europa, firmado el 28 de enero de 1981 y que en su artículo primero señala:

> El fin del presente convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona.

La protección del derecho a la intimidad resulta contemplada hasta en la Convención sobre los Derechos del niño del 20 de noviembre de 1989.

En el ámbito del derecho interno de los Estados, la Constitución de los Estados Unidos de América, en la primera y en la cuarta enmienda de 1791, consagra además del derecho a la libertad de expresión y el derecho a la libertad de prensa, la protección a las personas, casas, papeles y posesiones contra molestias sin la debida orden. En los Estados Unidos de América también se han promulgado diversas leyes tendientes a

tutelar la intimidad como derecho, así podemos mencionar: la *Bank Secrecy Act* de 1970, la *Electronic Communication Privacy Act*, la *Money Laundering Control Act*, la *Fair Credit Reporting Act* que es parte de la *Consumer Credit Protection Act*, la cual protege al consumidor de crédito en relación con las reglamentaciones de los institutos o compañías dedicadas a brindar informaciones de crédito y principalmente contra la *difamation, invasion of privacy, or negligence and regardless of how the information is stored* (como quiera que se recopile y conserve la información). También puede citarse la *Privacy Act* de 1974, la cual se aplica a los datos privados de las personas naturales almacenados en bancos de datos del gobierno, infiriéndose de la misma como sujetos activos de los ilícitos contra la intimidad informática, a los responsables de los bancos de datos y a los particulares o usuarios de los mismos. Esta *Privacy Act* tiene por finalidad directa, el proteger la vida privada y el reconocimiento del derecho de todo individuo para conocer las informaciones sobre su persona y para corregir aquellas erradas o relativas a informaciones no autorizadas.

La *Privacy Act* consagra gran parte de los principios para la protección de los datos personales que detallaremos más adelante, entre ellos, el de que los datos almacenados deben ser consecuentes con los fines para los cuales se creó la entidad que los recoge, que la información se recoja directamente de la persona a la que concierne, la actualización de los datos y la garantía del derecho de acceso. Aunque se establecen algunas restricciones en lo relacionado con las agencias de seguridad pública. También se señala que la difusión de tal información sólo será permitida en caso de autorización del interesado o en razón de orden de autoridad competente (Infra, pág. 148).

Cabe comentar que la *Freedom of Information Act* de 1966, la cual consagra el derecho de todo ciudadano al acceso de la información contenida en documentos públicos, o sea el derecho a la información, instituye como limitación de tal acceso, todo

lo concerniente a la vida privada de las personas, o sea hace prevalecer el derecho sobre la información.

El Estatuto Federal de Delito Informático de 1984 tipifica entre otros actos considerados como *computer crimes* y por lo tanto susceptibles de responsabilidad penal y civil, los siguientes:

La utilización desautorizada de un computador para obtener información financiera o de crédito, protegida por las leyes financieras privadas de carácter federal, tales como la Ley de Derecho a la Privacidad Financiera de 1978 y la Ley de Información del Crédito Equitativo.

También en el ámbito de la legislación estatal de los Estados Unidos cabe mencionar el Estatuto de California y la Ley 1305 del Estado de Florida aprobada en 1978 y la cual entre otras ofensas públicas y por lo tanto susceptibles de responsabilidad tanto penal y civil menciona las siguientes:

(1) Cualquiera que deseándolo, sabiéndolo y sin autorización modifique datos, programas o documentación de soportes (almacenada o existente, interna o externamente, en un computador, sistema o red de computadores), comete un daño contra la propiedad intelectual.

(2) Cualquiera que deseándolo, sabiéndolo y sin autorización acceda o permita el acceso a cualquier computador, sistema o red computacional, o niegue el acceso a los mismos, el cual corresponde a un usuario autorizado de tal servicio, al que le pertenece total o parcialmente bajo contrato, operado por, en representación de o junto con otros, comete una ofensa contra los usuarios computacionales.

(3) también se consideran ofensas criminales los actos anteriores cuando los mismos tengan por objeto la comisión de un fraude u obtener cualquier propiedad.

En Francia, además de la Ley 78-17, a la cual nos referiremos más adelante (Infra, pág. 162) , el Código Penal tipifica como ilícitos penales y por ende también

susceptibles de generar responsabilidad civil, conductas tales como: el acceso fraudulento a los sistemas de tratamiento automatizado de datos; la conservación fraudulenta de los datos; y, el sabotaje informático, o sea el impedir o alterar el funcionamiento de un sistema automatizado de datos.

Por otra parte la Constitución del Reino de los Países Bajos (Holanda) de 1983, incluye en su artículo décimo relativo a la intimidad personal: la obligación de legislar para la protección de "la esfera de la vida personal en relación con la acumulación y suministro de datos personales" así como sobre "la responsabilidad de las personas con ocasión del examen de los datos por ellas almacenados y del uso que hicieren de ellos así como el aprovechamiento de tales datos".

La Constitución argentina en su artículo 19 señala:

> Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios y exentas de la autoridad de los magistrados.

Por su parte el Código Civil argentino en su artículo 1071 bis, plantea en forma clara la responsabilidad civil en que incurre quien de alguna forma atenta contra el derecho a la intimidad de las personas. La disposición en referencia establece:

> El que arbitrariamente se entrometiere en la vida ajena publicando retratos, difundiendo correspondencia, mortificando a otro en sus costumbres o sentimientos o perturbando de cualquier modo su intimidad y el hecho no fuere un delito penal, será obligado a cesar en tales actividades si antes no hubiese cesado, y a pagar una indemnización que fijará equitativamente el juez, de acuerdo con las circunstancias; además podrá éste, a pedido del agraviado, ordenar la publicación de la sentencia en un diario o periódico del lugar, si esta medida fuese procedente para una adecuada reparación.

Además, en varias constituciones provinciales de la Argentina, se han introducido reformas sobre el tema de la informática y las libertades. Tal es el caso de la Constitución de la Rioja (1986), San Juan (1986) y Córdoba (1987), las cuales recogen los principios inspiradores de las legislaciones europeas y estadounidenses.

En España el artículo 18 de la Constitución garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen, así como el secreto de las comunicaciones y dispone que la ley limitará el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos.

Así también el Código Penal español, en su artículo 199 considera como un ilícito penal y por ende también susceptible de generar responsabilidad civil, el faltar a las prescripciones legales sobre la informática para grabar datos relativos al honor o la intimidad personal o familiar de terceros, o en perjuicio de los mismos manipular la información legítima o ilegítimamente procesada.

También podemos mencionar la Constitución chilena de 1980, la cual establece:

> La Constitución asegura a todas las personas:
> .....
> .....
> 4° El respeto y protección a la vida privada y pública y a la honra de la persona y de su familia.

Posteriormente se promulga el 5 de mayo de 1982, la ley orgánica constitucional sobre la protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

En Portugal, el artículo 35 de la Constitución, en lo que a la denominada intimidad informática se refiere, señala:

> 1. Todos los ciudadanos tendrán derecho a informarse del contenido de bancos de datos acerca de ellos y de la finalidad a que se destinen las informaciones y podrán

> exigir la rectificación de los datos, así como su actualización.
> 2. Los terceros tendrán prohibido el acceso a archivos con datos personales y a las interconexiones que surjan de ellos así como a los flujos de información transnacionales, salvo en casos excepcionales previstos por la ley.
> 3. No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos.
> 4. La ley determinará el concepto de datos personales para el propósito de bancos de datos.
> 5. Los ciudadanos no podrán recibir un número de identificación único usable para todo tipo de propósitos.

En el ámbito constitucional también puede mencionarse el artículo 15 de la Constitución turca, el artículo 45 de la Constitución egipcia de 1971, el artículo 28 de la constitución ecuatoriana de 1967.

En Alemania, se ha promulgado la Ley para la protección contra el uso ilícito de datos personales o *Datenschutz* de 27 de enero de 1977, la cual establece como su principal finalidad el impedir todo daño a los bienes dignos de tutela de los ciudadanos, protegiendo sus datos personales sobre los abusos de registro, transmisión, modificación y cancelación en la elaboración de las informaciones. Esta legislación incluye los bancos de datos públicos y los privados.

En México tenemos la Ley de Instituciones de Crédito, la cual consagra la institución del secreto bancario.

En el Reino Unido destaca la Ley de protección de datos de 1984.

También mantienen una legislación protectora de datos nominativos: Luxemburgo con la Ley reguladora de la utilización de datos nominativos en registro informáticos del 31 de marzo de 1979; Israel mediante la Ley 5714 del 23 de febrero de 1981, sobre protección de la privacidad y la Ley del 16 de marzo de 1981, sobre las

directrices aplicables al tratamiento de los datos personales en la Administración Federal e Islandia con la Ley sobre recolección de datos personales.

A nivel de Latinoamérica, tres países han elaborado recientemente proyectos de ley de carácter nacional para la protección de los datos personales, a saber: Argentina, Colombia y Chile. Estos proyectos se fundamentan en los principios que han inspirado ya los ordenamientos jurídicos existentes en Europa y los Estados Unidos.

(b) Contenido de la Legislación: la protección de la intimidad a través de la protección de los datos personales.

Todas estas disposiciones tienen en común su intensión en solucionar: "el conflicto de intereses que se plantea entre el derecho a la vida privada que tiene todo individuo y el derecho a la información, o la libertad de información que es la consecuencia de su ejercicio. Es decir, se procura lograr un equilibrio entre la información que necesita la sociedad para un funcionamiento democrático y el derecho del individuo a la protección de los datos que le conciernen" (Correa, 1987: 244).

Y es que el derecho a la libertad de expresión ha evolucionado hoy en día, hasta ser catalogado más bien como el derecho a la libre circulación de información o libertad de información, el cual conforme a los criterios del Consejo Económico y Social de las Naciones Unidas, descansa sobre tres bases fundamentales, a saber: la libertad de investigar o recabar información, la libertad de difundirla y la libertad de recibirla. Razón por la cual los legisladores nacionales e internacionales, al tutelar el legítimo interés a la intimidad de las personas han tenido que determinar los límites de estos derechos a fin de imponen un balance racional.

Las anteriores consideraciones, aunadas al desarrollo de la tecnología, sobre todo en el campo informático, han dado lugar a que surja en el derecho comparado la necesidad de proteger el legítimo interés a la intimidad pero bajo el concepto de la protección de los datos personales también llamados nominativos. Esta protección de los datos se fundamenta en el hecho de que actualmente el derecho a la vida privada no se concibe como una libertad negativa consistente en rechazar u oponerse al uso de información sobre sí mismo, sino en una la libertad positiva de supervisar el uso de la información.

En el ámbito del derecho comparado, se han utilizado sobre todo dos técnicas para regular la protección de los datos personales, a saber:

1. Las denominadas leyes "ómnibus" de naturaleza global y que han tenido su mayor difusión en los países europeos.

2. Las leyes que podríamos denominar como casuísticas, pues sólo regulan conflictos específicos y que han tenido su origen en los Estados Unidos de América.

No obstante lo anterior para Foyen (Foyen En: Jijena, 1992: 50-51), estas leyes se pueden clasificar en: (1) normas sustanciales combinadas con sanciones penales; (2) normas sustanciales combinadas con un *ombudsman* o defensor del pueblo para la protección de los derechos humanos en general o de los datos personales en particular; (3) normas sustanciales combinadas con una institución con poderes de decisión para la protección de los datos personales y la regulación de los bancos de datos.

Para Rodotá (Rodotá En: Correa, 1987: 252), una legislación adecuada sobre esta materia debería contar con los elementos siguientes:

(1) una ley básica con principios generales;

(2) normas específicas para regular los conflictos planteados en determinados sectores;

(3) un órgano independiente para la supervisión y reglamentación;

(4) la intervención del poder judicial por vía de apelación;

(5) la articulación de la supervisión de forma extensa.

Se habla inclusive de la existencia de una nueva libertad fundamental, o sea la libertad informática, definida como: "el derecho de disponer de la información, de preservar la propia identidad informática, o lo que es lo mismo, de consentir, controlar, rectificar los datos informativos concernientes a la propia personalidad" (Frosini, 1988: 35).

En cuanto al control de la información, éste puede corresponder a la persona o al Estado por vía de una Legislación administrativa. A nosotros nos interesa más que nada, el primero, pues el no reconocimiento del derecho de control por parte de las personas sobre la información que les concierne, es lo que hará susceptible la irrogación de un daño y la consecuente responsabilidad civil para quien lo ocasiona.

En el derecho comparado se reconocen a todas las personas, la facultad de ejercer derechos de control sobre el tratamiento electrónico de los datos que le son inherentes. A estos derechos se les han denominado derechos de acceso. Con relación a estos derechos, sobre los cuales ya hicimos una breve referencia, al comentar sobre la intimidad y la informática bancaria (Supra, pág. 148), pero que cobran especial relevancia en razón del interés de la Legislación Comparada en la protección de los datos personales, Foyen señala que una adecuada normativa debe contemplar cinco intereses fundamentales, a saber:

(1). El interés sobre la confidencialidad. El sujeto de los datos puede estar interesado en que determinada información que él considere relevante no se dé a conocer.

(2). Interés en que los datos sean completados y actualizados.

(3). Interés de estar informado acerca de lo que pretende hacer con los datos.

(4) Interés en contar con una administración eficiente.

(5) Interés en que los datos no sean usados de manera ilícita (Foyen, En: Correa, 1987: 253).

Para la Doctrina, además de reconocerse el derecho de acceso, se necesita garantizar el mismo, proporcionando información a la persona sobre la existencia de bancos de datos, el tipo de datos que contienen y las posibilidades de consultar el mismo. También, se requiere la existencia de órganos que controlen la actuación de los bancos de datos bajo la forma de entidades públicas o privadas, con el fin de que velen por el reconocimiento del derecho de acceso.

En cuanto a las personas que deberían gozar de este derecho de acceso, se propone que el mismo se reconozca tanto a las personas naturales como a las personas jurídicas o morales, con lo cual se amplía a nuestro juicio, el concepto tradicional de intimidad como un derecho único de las personas naturales o físicas. Además, se considera que este derecho puede ser ejercido tanto frente a entidades públicas como a entidades privadas. Nosotros consideramos convenientes ambas posiciones, toda vez que los daños morales o inmateriales y los daños materiales indirectos pueden afectar los intereses legítimos tanto de las personas naturales como de las jurídicas e inclusive en algunos casos la lesión puede ser más grave tratándose de las personas jurídicas, las cuales tienen una clientela frente a la cual mantener su credibilidad y prestigio. También es un hecho cierto que tanto el Estado como los particulares en su condición de

administradores de bancos de datos, tienen iguales posibilidades de menoscabar los legítimos intereses de las personas cuya información se encuentra registrada en el cerebro electrónico de las mismas.

A pesar de que Suecia promulgó una Ley el 1 de julio de 1973, la primera en el mundo en su campo, también conocida como la *Datalag*, y que contempló la autorización previa para la creación de bancos de datos, el derecho de acceso y la creación de un órgano de control administrativo y que Alemania hizo lo propio en 1977, se afirma que las legislaciones sobre protección de datos personales aprobadas en: Austria, Dinamarca (leyes 243 y 244 del 8 de junio de 1978), Francia (Ley No. 78-17 sobre informática, ficheros y libertades del 6 de enero de 1978) y Noruega ((Ley 48 de 9 de junio de 1978), son los ejemplos más acabados sobre legislaciones de datos personales.

Estas recogen diez principios (Correa, 1987: 257 a 261) que pueden ser detallados como sigue:

(1) El principio de justificación social, conforme al cual la captación de datos debe tener un objetivo general y usos determinados y aceptados por la sociedad (Artículo 1 de la Ley francesa, 17 de la Ley austríaca, 3 de la Ley danesa sobre registros privados y 9 de la Ley danesa de registros públicos y 6 de la Ley noruega).

(2) El principio de la limitación de la recolección, conforme al cual la información debe ser recolectada por medios lícitos, o sea con conocimiento y consentimiento de las personas a las que la misma les es inherente o con autorización legal, y siempre que se limiten a aquella que es suficiente para cumplir con la finalidad perseguida, lo cual implica que no puede haber de por medio ni engaños, ni ocultamientos de la finalidad de la recolección (Artículo 3 de la Ley danesa de registro privados, 9 de la Ley danesa de autoridades públicas, 25 y 31 de la Ley francesa y 6 de la Ley noruega). Cabe advertir que el autor francés Weill, reconoce la existencia de un

derecho de oposición al tratamiento de los datos, por razones legítimas, en virtud de lo que él considera: "la idea subyacente en la ley de un dominio de los individuos sobre los datos nominativos que le conciernan" (Jijena, 1992: 50).

(3) Principio de la calidad o fidelidad de la información, conforme al cual los datos personales que se recolecten y almacenen deben ser exactos, completos y actuales, de tal forma que los mismos no den lugar a que se concluyan errores. Lo anterior implica que estas leyes reconocen el derecho de los interesados a rectificar, cancelar o actualizar cualquier información inexacta o incompleta, en lo que se conoce como el derecho de acceso y de rectificación (artículo 26 de la Ley austríaca, 6 de la Ley danesa de registros privados, 11 de la Ley danesa de autoridades públicas, 37 de la Ley francesa y 8 de la Ley noruega).

(4) Principio de la especificación del propósito o la finalidad, conforme al cual los fines u objetivos para los cuales se recolectan los datos deben estar especificados al momento de tal recolección, sin que se puedan utilizar para fines distintos (artículo 8 de la Ley austríaca, artículo 20 de la ley danesa de autoridades públicas, artículo 19 de la ley francesa y artículo 11 de la ley noruega).

Se comenta que este principio resulta vinculado directamente con el respeto a la dignidad del hombre, ya que quien es indagado debe conocer el fin de la utilización de los datos que suministra y que luego exista un control que permita conocer si fueron realizados tales fines (Parellada, 1990: 364).

(5) Principio de la confidencialidad, en virtud del cual el acceso a los datos por parte de terceras personas requiere consentimiento del titular de tales datos o de autorización legal (artículos 7, incs. 1 y 2 de la ley austríaca; 4 de la ley danesa de registros privados y 16 y 17 de la ley danesa de autoridades públicas; 43 de la ley francesa).

(6) Principio de salvaguarda de la seguridad, el cual establece que la institución o entidad que se responsabiliza por el registro o banco de datos personales, tiene la obligación de tomar las medidas de seguridad necesarias para protegerlos contra pérdidas, destrucciones o acceso no autorizado (Supra, pág. 115) (artículos 21 de la ley austríaca, 6 de la ley danesa de registros privados, 12 de la ley danesa de autoridades públicas, 21 y 29 de la ley francesa y 24 de la ley noruega). Estas obligaciones, en nuestra opinión, son de medios y no de resultados, ya que la Ley exige la adopción de lo que denomina precausiones útiles (Jijena, 1992: 49).

Lo anterior implica que las entidades bancarias deben de proveerse de los denominados *software* de seguridad con la finalidad de cumplir con la obligación de salvaguarda de la intimidad de su cliente y también en función del típico principio de reserva bancaria. Esto pues, aparte de que lo autorice el propio cliente, el banco sólo puede consentir una intromisión en los datos de sus clientes cuando ello sea justificado por la defensa o garantía de un interés público prevaleciente.

(7) Principio de apertura, por medio del cual se garantiza la transparencia de los actos de las entidades estatales y de la empresa privada con relación a los procedimientos, desarrollo y prácticas relativas al procesamiento electrónico de datos personales. Para garantizar la efectividad de este principio, los particulares deben conocer la existencia, fines, usos y métodos utilizados en la operación de los registros o bancos de datos personales (artículos 14 de la ley austríaca, 22 de la ley francesa y 8 de la ley danesa de autoridades públicas).

Cabe advertir que la transparencia informática a la que se hace referencia con este principio, implica que el programa informático debe ser comprobable y controlable durante el procesamiento de los datos.

(8) Principio de la limitación en el tiempo, el cual señala que los datos no deben ser almacenados en el registro o la memoria del computador, sino sólo por el tiempo

requerido para alcanzar los fines para los cuales los mismos fueron recolectados (artículos 27 de la ley austríaca, 6 de la ley danesa de registros privados, 5 de la ley danesa de registros públicos, 28 de la ley francesa y 11 de la ley noruega).

(9) Principio de control, en atención al cual debe establecerse un ente de control para garantizar la observación de los principios antes mencionados o los que se establezcan en la legislación interna de cada país (artículos 22 de la ley danesa de registros de autoridades públicas, 6 de la ley francesa, 2 de la ley noruega y 35 de la ley austríaca).

(10) Principio de la participación individual, según el cual todo individuo debe tener el derecho de acceso a los datos que le son propios y los cuales se reflejan en las siguientes facultades:

a) conseguir de la persona responsable del registro o bancos de datos, detalles de la información personal del interesado;

b) que dicha información sea suministrada en un término razonable y que la misma sea comprensible para el solicitante;

c) que se le reconozca el derecho de objetar cualquiera de los datos personales almacenados y que tal objeción quede consignada;

d) que en virtud de la mencionada objeción y de estar esta debidamente fundamentada, tales datos personales sean borrados del registro o la memoria del computador, o bien corregidos, completados o aclarados;

e) que se le informe de los motivos para no admitir su derecho de acceso o su reconocimiento en lugar, tiempo y forma razonables;

f) objetar el rechazo de motivar la negativa a reconocer el derecho de acceso.

Sobre este último principio la ley francesa señala:

> Toda persona que acreditare su identidad, tendrá derecho a acudir a los servicios u organismos encargados de llevar a cabo los tratamientos automatizados cuya lista fuere accesible al público en virtud de lo dispuesto en el artículo 22, con miras a saber si tales tratamientos hacen referencia a informaciones nominativas que le afectaren y, en tal caso, para que le fueren comunicadas (artículo 34).
> Se expedirá copia al titular del derecho de acceso que la solicitare, previo el abono de una tasa global variable en función del tipo de tratamiento, y cuyo importe será fijado por resolución de la Comisión y homologado por orden del ministro de Economía y Hacienda....(artículo 35).
> El titular del derecho de acceso podrá exigir que las informaciones que le afectaren y fueren inexactas, incompletas, equívocas, caducas o cuya colecta, utilización, comunicación y conservación estuviera prohibida, sean rectificadas, completadas, aclaradas, actualizadas o canceladas.
> Cuando el interesado así lo solicitare, el servicio u organismo correspondiente deberá expedir gratuitamente copia del registro debidamente modificado.
> En caso de impugnación la carga de la prueba incumbirá al servicio ante el cual hubiere sido ejercido el derecho de acceso, a menos que quedare probado que las informaciones impugnadas habían sido comunicadas por la persona afectada o con su conformidad (artículo 36).

Se señala que estos principios generales de protección de datos en que se fundamenta la mayor parte del derecho positivo foráneo, deben ser considerados como parte fundamental del derecho informático y por ende de la relación banco - cliente en lo que la novísima disciplina le resulta aplicable.

Por otra parte, cabe advertir que estos principios pretenden proteger los datos personales en cada una de las fases principales del ciclo operativo de la automatización informática, a saber: la recopilación de los datos (principio de justificación social, limitación de la recolección, calidad o fidelidad de la información, propósito), el procesamiento (principio de seguridad y apertura), el resultado obtenido y puesto a disposición (principio de control, de limitación en el tiempo y de participación

individual) y su transmisión en redes informáticas y su difusión (principio de confidencialidad).

Finalmente, hay que señalar que ya se habla de leyes de la primera y de la segunda generación en materia informática, estas últimas referidas a las legislaciones que empiezan a ser promulgadas con la finalidad de adecuarse a los nuevos cambios tecnológicos y cuya primera finalidad resulta ser reformar las leyes expedidas originalmente en Europa y Estados Unidos, en los inicios de los años setenta. En adición, hay que advertir que las nuevas leyes de datos tienden a proteger también, la información electrónicamente tratada de las personas jurídicas o morales que con anterioridad quedan excluidas del ámbito de aplicación de este tipo de legislaciones.

(c) Tratamiento del tema por parte de los organismos internacionales.

La Organización de las Naciones Unidas a tratado el tema de la informática y el derecho a la intimidad en diversas conferencias. Así la Conferencia Internacional de Derechos Humanos de Teherán expresó su preocupación por la posible violación de los derechos humanos a través del uso de la informática, específicamente se manifestó la preocupación por las aplicaciones de la electrónica que afecten los derechos de la persona y los límites que en tal sentido deberían aplicarse. Por su parte la Secretaría General en un estudio elaborado entre 1973 y 1976, planteó los riesgos del registro computarizado de datos personales, sobre todo en razón de un posible acceso indiscriminado de la información, el aumento de los errores en los datos que se almacenen con motivo de fallas técnicas o de programación, razones por las cuales son

necesarias medidas físicas, técnicas y jurídicas que garanticen el uso de tal tecnología sin que ello implique una violación a los derechos humanos.

En 1983, la Sub-Comisión de lucha contra las medidas discriminatorias y protección de la minoridad de la Comisión de Derechos Humanos de la O.N.U., inició la elaboración de un estudio para la determinación de los principios aplicables a los bancos de datos personales. De tal forma el 29 de agosto de 1984, elaboró un anteproyecto de principios aplicables al manejo de bancos de datos, entre los cuales señaló los de la licitud y honestidad de los procedimientos, la determinación y justificación de los fines, la exactitud de la información, el derecho de acceso y la no discriminación (Correa, 1987: 263 a 264).

Por su parte el Consejo de Europa elaboró resoluciones sobre la protección de la vida privada de las personas naturales con relación a los bancos de datos electrónicos en el sector privado y en el sector público en 1973 y 1974, respectivamente. Estas resoluciones recomendaban a los Estados la adopción legislativa de los principios para la protección de los datos personales a los que ya nos hemos referido (Supra, pág. 162). El 22 de setiembre de 1980, el Consejo de Europa adopta la Convención para la protección de los individuos con relación al procesamiento automático de datos personales, la cual convierte en normas de derecho internacional, los principios para la protección de los datos personales, ya mencionados, y establece disposiciones relativas al denominado flujo de datos transfronteras. También dentro del ámbito del Consejo de Europa se aprueba el 28 de enero de 1981, el Convenio de Estrasburgo para la protección de las personas respecto del tratamiento automatizado de datos de carácter personal.

Por otra parte el Proyecto de Directiva del Consejo de la Comunidad Económica Europea sobre el consumidor y los medios modernos de pago, establece en su artículo sexto, que los Estados miembros deberán asegurar que:

> a) Las redes de transferencias electrónicas de fondos produzcan registros suficientes para permitir que las transacciones sean rastreadas y los errores rectificados.
> b) En cualquier disputa referente al uso de la tarjeta o la operación de sistema, la carga de la prueba recaerá sobre el emisor de aquella, el que deberá demostrar que la transacción fue debidamente registrada y no fue afectada por ningún desperfecto técnico u otra deficiencia, poniendo a disposición de la otra parte, sus libros, registros, cintas y otros medios probatorios.
> c) Se provea al cliente, si así lo requiriese, registros escritos de cada transacción, ya sea en el momento o poco después de haberse efectuado (Delpiazzo, En: Del Moral, 1996c: 24).

La Organización de Cooperación y Desarrollo Económico (OCDE) ha buscado fundamentalmente, que se respete el libre derecho a la circulación internacional de los datos personales. Este aspecto del problema es relevante si se toman en cuenta las diferencias existentes en las legislaciones de los distintos estados, además de la inclusión en varios de ellos del principio de reciprocidad para la protección de los datos personales y algunos otros incluyen limitaciones basadas en cuestiones de seguridad nacional. Por tal razón, la OCDE aprobó en 1980, un documento denominado Lineamientos para regular la protección de la vida privada y el flujo transfrontera de datos personales, en el cual se recomienda la adopción de los principios para la protección de los datos personales antes detallados.

3. Limitaciones al derecho a la intimidad en la informática bancaria.

Lógicamente que existirán limitaciones que afectarán el derecho a lo que podríamos denominar, la intimidad bancaria. Estos serán en términos generales coincidentes con las limitaciones existentes en cuanto al secreto bancario (Supra, pág.

57). Fundamentalmente el interés privado que se refleja en el caso del derecho a la intimidad deberá ceder frente al interés público. Es así que aún siendo confidencial la información registrada por medios electrónicos, las autoridades competentes -esencialmente las jurisdiccionales- que invoquen un interés público legalmente reconocido, tendrán plena facultad para requerir de las entidades bancarias, cualquier información necesaria y pertinentes para el cumplimiento de los fines para los cuales éstas han sido constituidas y los bancos están en el deber de revelar a dichas autoridades tales datos o informaciones.

A lo anterior debemos añadir, lo relativo al intercambio de información crediticia interbancaria para los efectos de medir el riesgo de los créditos que otorga el banco. En muchas legislaciones sobre todo de América Latina, el banco de datos sobre información crediticia de las personas, conocido en algunos casos como Central de Riesgos (Glen, 1983: 130), constituyen una excepción expresa al principio de reserva o secreto bancario y como consecuencia lógica del derecho a la intimidad. Sin embargo lo anterior no implica que el banco no será responsable cuando la información que revele a la central de riesgos o banco de datos crediticios, resulte ser equivocada o exagerada, causando perjuicios al potencial usuario del crédito. Ello es así puesto que, en estos casos, el banco incurrirá en responsabilidad civil extracontractual frente al perjudicado por el daño causado a su buen nombre, o sea, a su honor e inclusive a su patrimonio por la posible pérdida de un chance.

En Colombia, la jurisprudencia más reciente analiza el caso de las centrales de riesgo en el fallo de 1 de marzo de 1995 de la Corte Constitucional, en el caso Gabriel Alberto González Mazo contra DATACREDITO de COMPUTEC. En este caso, la parte actora había solicitado un crédito en 1990 a Invercrédito Servicios Financieros, S. A. Con motivo de un atraso en los pagos de dicho crédito el Sr. González fue registrado como deudor moroso a la División DATACREDITO de la Compañía Computec, S. A.

(para nuestros efectos la Central de Riesgo). El demandante pagó su deuda y su paz y salvo se le entregó el 25 de junio de 1993. Sin embargo, su nombre aún aparecía en el archivo de la demandada al momento de presentar la demanda, bajo la clasificación de cartera recuperada. En tal virtud el demandante no había podido ser sujeto de ningún crédito, ni tampoco constituirse en garante personal de terceros ante ninguna entidad crediticia.

La parte actora solicitó la tutela del derecho a la intimidad consagrado en el artículo 15 de la Constitución colombiana.

En lo que al presente estudio interesa, la Corte se pronunció sobre el recurso del *hábeas data*: su contenido y los medios jurídicos para su protección.

En razón de lo anterior la Corte inicia por reconocer el reconocimiento constitucional que en Colombia tiene la institución jurídica del *hábeas data*, a partir del artículo 15 de su Carta Magna, el cual establece: "De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas".

El *hábeas data*, a juicio de la Corte, está integrado por el derecho a la autodeterminación informática y por la libertad en general, y en especial económica. Tal autodeterminación, según la Corte, es la facultad de la persona a la cual hacen referencia los datos, para los efectos de autorizar su conservación, uso y circulación, de conformidad con las regulaciones legales.

El sujeto activo de la mencionada autodeterminación lo es toda persona física (natural) o jurídica, cuyos datos personales sean susceptibles de tratamiento automatizado.

Por otra parte, el sujeto pasivo es toda persona física (natural) o jurídica que utilice sistemas informáticos para la conservación, uso y circulación de datos personales. Estos últimos datos, para los efectos del caso en comento, incluyeron los

relativos a la capacidad económica de la persona y en lo específico, a la manera como ella atiende sus obligaciones económicas para con las instituciones de crédito.

El contenido del *hábeas data* incluye tres facultades, según la Corte, a saber:

a) El derecho a conocer las informaciones que a ella se refieren (derecho de acceso);

b) El derecho a actualizar tales informaciones, es decir, a ponerlas al día, agregándole los nuevos hechos (derecho de rectificación);

c) El derecho a rectificar las informaciones que no correspondan a la verdad (es parte también del derecho de rectificación).

A los tres anteriores pueden adicionarse, el derecho a la caducidad del dato negativo, el cual si bien no consagra la disposición constitucional, sí puede inferirse de aquella; además la doctrina reconoce como parte de esta institución, el derecho de oposición a la recolección de ciertos datos, los considerados sensibles.

Igualmente se reconoce el derecho de toda persona para solicitar la actualización y rectificación de los datos no congruentes con la verdad, a quien maneja el banco de datos, y además para exigir la adopción de tales medidas, en caso de que su solicitud no sea acogida. Pero para ejercer tal derecho, la persona tiene también uno previo, cual es el que se le dé a conocer la inclusión de la información que le concierne en un banco de datos.

La institución del *hábeas data* guarda también relación según el fallo, con la forma como se manejan los datos. Al respecto el precitado artículo 15 dispone: "En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Cónstitución".

En consecuencia con lo anterior, los datos obtenidos por medios ilícitos, no pueden ser almacenados en un banco de datos. A esto se suma el hecho de que no se podrán almacenar datos relativos a la esfera íntima de las personas (datos sensibles), los

cuales si fueren incluidos en un banco de datos, deberán ser excluidos ante una simple petición del afectado, quien también tendrá el derecho a la acción de tutela en salvaguarda de sus derechos.

En otro aspecto de suma importancia en lo que a nuestro estudio se refiere, la Corte se hace unas interrogantes, las cuales contesta, acto seguido, con inigualable brillantes. Tales interrogantes son: ¿Existe un derecho de los establecimientos de crédito a recibir información veraz sobre la conducta de sus posibles deudores en lo tocante al cumplimiento de sus obligaciones? ¿Tiene el deudor derecho a impedir que el acreedor informe sobre la manera como él cumplió o cumple sus obligaciones?

En este sentido la mencionada corporación de justicia responde sobre la base de los siguientes razonamientos:

(a) Las instituciones de crédito por manejar el ahorro público ejercen una actividad de interés general.

(b) Tales instituciones no pueden prestar sus servicios, ni otorgar créditos, a personas desconocidas.

(c) El prudente manejo bancario indica que todo banco debe obtener información que le permita determinar la suerte que correrán los dineros concedidos en préstamo.

(d) La obtención de información sobre sus posibles prestatarios constituye una actividad de defensa de los intereses institucionales, que en definitiva son los intereses de sus depositantes. Esto es lo que el alemán Denninger denomina la previsión informativa (Denninger, 1987: 269), en virtud de la cual ciertas instituciones sólo pueden cumplir con sus fines, contando con la información que les haga falta.

(e) El deudor no tiene derecho a impedir el suministro de información, en virtud de:

1. Que la información versa sobre hechos no sólo relacionados con el deudor.

2. Que el deudor no puede impedir a la institución el ejercicio de un derecho que le es propio.

3. Que la información versa sobre hechos no relacionados directamente con su intimidad.

No obstante, debe advertirse que los supuestos anteriores se asientan en el presupuesto de que el cliente ha autorizado la revelación de la información, o sea que debe primar el denominado principio de autorización previa.

Sobre este último principio, al cual ya hemos hecho referencia (Supra, págs. 148, 163), se dice que la autorización debe ser expresa y voluntaria por parte del interesado para que sea eficaz, pues en caso contrario no se haría uso efectivo de tal derecho. Además el cliente debe conocer de antemano y en forma clara, las consecuencias de tal autorización.

Cabe advertir que otros autores como Parellada (Parellada, 1990: 246), señalan que los datos relativos al incumplimiento de las obligaciones asumidas y que denominan datos negativos, no resultan protegidos por la legislación protectora de la intimidad o la que instituye el secreto bancario. Ello es así por cuanto que el incumplimiento es un acto que se realiza frente a terceros y por lo tanto fuera del ámbito de la intimidad.

También se entró al análisis de la amplitud de la información de crédito que puede ser revelada. ¿Debe sólo revelarse si la persona es o no deudora? ¿Debe revelarse sólo si el deudor esta o no en mora al momento de referirse la información? La respuesta que se da a estos cuestionamientos es que la información además de veraz debe ser completa. Así tratándose de un crédito, un banco no da una información completa cuando se limita a expresar que un deudor no debe nada, sin advertir que la

cancelación del crédito fue el resultado de un proceso judicial, o que la deuda estuvo morosa por largo tiempo. Además, la información para ser completa debe indicar el momento en el que el cliente se puso a paz y salvo.

Se señala que incurre en culpa el funcionario bancario a cargo del otorgamiento de créditos, que al analizar el riesgo de la operación, no examina los antecedentes crediticios del posible deudor y su incidencia en el grado de riesgo del crédito.

En adición a lo anterior, también se señala que si bien el deudor tiene derecho a que la información sobre su persona se actualice, ello no implica un derecho a suprimir el pasado, a suprimir los antecedentes de tal deudor. Actualizar quiere decir registrar, agregar un hecho nuevo. Tratándose de un deudor moroso que al fin de cuentas paga, ya sea de forma voluntaria o compulsiva, su registro como deudor debe incluir toda la información, incluyendo la fecha del pago como un nuevo hecho. Como dice la Corte: "Sostener lo contrario llevaría al absurdo de afirmar que actualizar una historia, es consignar únicamente el último episodio, eliminando todo lo anterior".

Además se afirma que la revelación de la conducta crediticia de un cliente no es una sanción, bajo condiciones normales, sino el ejercicio del derecho fundamental a informar y recibir información veraz e imparcial.

Se analiza el aspecto del derecho a la información y el derecho a la igualdad de los deudores como parte de los razonamientos para decidir el caso en referencia.

En relación con lo anterior, se expresa que en presencia de dos deudores, uno cumplidor y el otro moroso, siendo que éste último sólo ha pagado en virtud de un proceso de ejecución, se viola el derecho a la igualdad, cuando a los dos se les crea un mismo perfil, dando una referencia de crédito que sólo exprese que ambos nada deben. Por ello el deudor cumplidor, en función de la defensa de su buen nombre, tiene el derecho a que se diga que cumplió oportunamente sus obligaciones.

Por todo lo expuesto, no se puede señalar que el revelar información crediticia negativa sobre un cliente, viola su derecho al buen nombre.

También se analiza el principio de limitación temporal de la información, es decir, la caducidad de los datos, o como ya hemos mencionado, el derecho al perdón o al olvido.

Igualmente se expresa que así como el deudor tiene derecho a que la información se actualice, a que la misma contenga hechos nuevos y positivos para el deudor, también hacia el pasado debe fijarse un límite razonable. Y surge la interrogante sobre: ¿qué ocurre en este caso?. Pues bien, se dice que el deudor luego de pagar sus deudas y haber tenido un buen comportamiento por un tiempo determinado y razonable, ha creado un buen nombre, una buena fama que en el pasado no tenía. Este tiempo determinado y razonable debe darlo la ley, no obstante aun si ello no es así, o sea si la ley nada dice, debe considerarse un término que evite el abuso del poder informático y preserve las sanas prácticas crediticias, todo ello en defensa del interés general.

Correlativamente con lo anterior, se propone como irrazonable, la conservación, el uso y la divulgación informática del dato, sin tomar en cuenta hechos tales como:

1. Un pago voluntario de la obligación.

2. El transcurso de un término de dos años, el cual es considerado como razonable, y el que debe contarse a partir del pago voluntario. Si la mora fuese inferior a un año, el término de caducidad debe ser igual al doble de la misma mora.

3. Que durante el término señalado en el párrafo anterior, no se hayan reportado nuevos incumplimientos del mismo deudor, en relación con otras obligaciones.

Se señala que si el pago ha sido el resultado de un proceso ejecutivo, aun a pesar del carácter público del mismo, la caducidad debería tener un término similar al de la prescripción de la obligación, o sea de cinco años.

La llamada caducidad del dato, se sustenta además en el hecho de que así como los que incurren en delitos o asumen obligaciones civiles, pueden ser rehabilitados, por qué no puede tener un límite temporal el dato financiero negativo.

Ahora bien, como resulta lógico suponer, tal caducidad debe estar sujeta a hechos o conductas del deudor que interrumpan la misma o que imposibilitan su efectividad. Por ello, si dentro del término de caducidad, ingresan al banco de datos otras informaciones sobre incumplimientos y mora de las obligaciones del mismo deudor o si hay un proceso judicial en su contra, dicho término no correrá o sencillamente se interrumpirá. Ello es así porque en tales casos no ha habido una reconstrucción del buen nombre comercial.

Estos razonamientos son consecuentes con el hecho de que el banco de datos debe cumplir la finalidad de informar verazmente sobre el perfil de riesgo de los usuarios del sistema financiero.

El término de caducidad se debe fijar en dos años, si el deudor paga la totalidad del crédito, únicamente con el hecho de ser notificado de la demanda.

Por otra parte, debe quedar claro que si el demandado en un proceso ejecutivo invoca excepciones y logra probarlas y que le sean reconocidas por el tribunal, los datos negativos que sobre tal crédito se encuentren en el banco de datos deben ser borrados. Únicamente deben exceptuarse los casos en los cuales la excepción probada y reconocida sea la de prescripción, pues en tal caso no ha habido pago, además del carácter público del dato.

Se concluye, entre otras cosas, que para que el crédito opere normalmente resulta preciso que exista confianza pública, la cual sólo se obtiene si se permite la circulación de información veraz sobre las personas en su papel de deudores.

A lo anterior se agrega el hecho de que las informaciones que revela una entidad acreedora, no imponen la obligación de decidir sólo sobre ellas. Estas informaciones son sólo datos que relacionados con otros, permitirán apreciar el riesgo que implica la concesión del crédito.

C. El secreto o reserva.

Si bien a la reserva o secreto bancario algunos le han atribuido generalmente una autonomía como bien jurídico protegido, lo cierto es que dicha característica resulta cuestionada cuando en ámbitos como el de la legislación penal, la misma resulta subsumida dentro del concepto de secreto profesional. A nivel de la doctrina y la legislación informática, la autonomía de la reserva o secreto bancario tanto como su propia existencia también resultan cuestionables por el reconocimiento efectivo de otros bienes jurídicos que por su amplitud parecen absorverlo. Y es que con el surgimiento de legislaciones nacionales e internacionales que durante el presente siglo, tutelan el bien jurídico intimidad, así como el desarrollo conceptual del mismo, el cual como ya señalamos (Supra, pág. 146), partió de una perspectiva negativa, o sea el derecho de estar sólo, el derecho de mantener cierta información que nos concierne en total reserva, sin que sea divulgada o revelada, pasando a ser en forma positiva, el derecho de controlar la información que nos concierne, el secreto bancario pareciera destinado de alguna forma ha ser absorbido por el bien jurídico intimidad. Ya vimos como doctrinalmente el secreto o reserva de la información resulta ser uno de los elementos

constitutivos de la intimidad, también resulta relevante el hecho de que en Europa se haya legislado para proteger los derechos sobre la información tanto de las personas naturales o jurídicas mediante una legislación única, superando la tradicional identificación del concepto intimidad con las personas naturales, al concluirse que las personas jurídicas también tienen derecho al control de la información que les concierne, así como el hecho de que si bien existe un derecho del titular de la información a decidir cuándo y a quienes se revelará una información, también existe el deber de las instituciones que mantienen dicha información almacenada aun mediante medios electrónicos, a no revelarla sino media tal autorización.

Por todo lo anterior, resulta evidente el hecho de que a la reserva o secreto bancario, en el ámbito informático al menos, deben serle aplicados los mismos principios a los que hicimos alusión tratándose del secreto o reserva como elemento constitutivo del bien jurídico intimidad, sin perjuicio de aquellos a los cuales hicimos alusión en el capítulo primero al desarrollar la institución del secreto bancario como característica de la actividad bancaria (Supra, pág. 55).

D. El honor.

El honor es un bien jurídico protegido que conforme a Borda puede definirse como: "el derecho a la consideración social, al buen nombre, al respeto y aprecio de terceros, a tener conciencia de la propia dignidad" (Borda, 1990: 329). Al decir de Zannoni (Zannoni, 1993: 253), dicho bien jurídico se compone de dos aspectos, a saber: el subjetivo, representado por un sentimiento a una dignidad moral propia que nace de las virtudes, méritos y valor moral de cada cual; y el objetivo, representado por

la evaluación que los demás realizan de nuestras cualidades morales y nuestro valor social, o lo que es lo mismo, la buena reputación. Pues bien, cuando como resultado de la información sobre sus clientes almacenada por una entidad bancaria en un banco de datos, resulta una mala referencia, la cual puede ser informada a otra entidad bancaria o a una central de riesgos, el buen nombre, el valor moral y la buena reputación del cliente va a sufrir un fuerte menoscabo importante por no decir desbastador. El hecho de que una persona sea identificada como mal sujeto de crédito o mal manejador de sus cuentas corrientes o de otra naturaleza, va a significar en muchos casos que dicha persona no pueda acceder a los servicios bancarios en largo tiempo, por no decir en forma indefinida, pues nuestra legislación no reconoce ni la caducidad del dato reflejado en las malas referencias crediticias, ni mucho menos conceptos como el derecho al perdón o al olvido, que en materia crediticia son instituciones desconocidas en nuestro medio, en el que el mal sujeto de crédito es poco menos que un leproso para los bancos. Por ello el daño, en estos casos, resulta evidente. Ahora bien habrá que definir si la mala referencia se refiere a la conducta irresponsable o negligente del propio cliente, en cuyo caso el banco no resulta responsable de dicho daño. Pero si la mala referencia es el resultado de un error de la entidad bancaria, en el procesamiento de los datos, al atribuir a una persona referencias que corresponden a otra; o por malas aplicaciones de los pagos efectuados a un préstamo o una línea de crédito; o por errores en la calificación de un crédito o la injustificada y desproporcionada ponderación de incumplimientos aislados que no permiten concluir una conducta reiterada o la determinación de un mal perfil, por un error de juicio en la evaluación del cliente, entonces el banco ha causado un indiscutible daño a su cliente, que aun ante la inexistencia de una legislación que reconozca la responsabilidad objetiva, será responsable porque ha habido culpa e inclusive de carácter grave, si se prueba la

intención del banco de causar daño o de no evitarlo habiéndolo podido hacer. Aquí la responsabilidad puede extenderse no sólo a un simple daño moral, sino también a un daño patrimonial indirecto, si como resultado de la afectación del bien jurídico honor se lesiona un interés patrimonial, como resulta de la imposibilidad de acceder a los servicios bancarios ante la consideración de mal cliente que refleja el sistema informático.

E. La identidad personal.

El denominado derecho a la identidad o personalidad de los individuos para algunos forma parte del bien jurídico intimidad y para otros tiene un carácter autónomo En nuestro caso y con la finalidad de dar una mejor explicación nos inclinaremos por considerarlo como un bien jurídico autónomo. Sin embargo, lo cierto es que éste es también un derecho personalísimo y conjuntamente con el derecho a la intimidad es considerado un derecho-garantía, ya que como señala Parellada: ".....presupuestan la vigencia efectiva de la libertad personal, son un medio de resguardo de la esencia de la persona humana, que es su libertad" (Parellada, 1990: 351).

La identidad o personalidad esta constituida por aquella información que individualiza a una persona y que por lo tanto nos permite diferenciarla de las demás (Ejemplo: el nombre, la edad, el estado civil, sus características físicas, su profesión, su estado de salud, así como su situación patrimonial e ingresos económicos) y la cual, como bien jurídico protegido, se instituye en función de la protección del patrimonio ideológico-cultural considerado en su máxima amplitud, no ya como esfera propia e íntima, reservada, sino en lo que atañe a la proyección social de la persona (Ibidem,

345 a 346). La información inherente a tal identidad resulta también conocida como información nominativa, la cual la ley francesa de 1978 define como:

> La información que permite la identificación de las personas físicas mediante el tratamiento automatizado de datos, y consiste en el conjunto de operaciones realizadas por medios automáticos de recolección, registro, modificación, conservación y destrucción de datos. Comprende también las operaciones que se refieren a explotación de ficheros o bancos de datos, especialmente las interconexiones, consultas o comunicaciones de aquellas informaciones nominativas así obtenidas.

Esta información nominativa puede resultar distorsionada por el mal uso de los sistemas informáticos y en nuestro caso, por los errores en que incurran las entidades bancarias en el procesamiento de la información proporcionada por sus clientes o en el mal uso que se haga de la misma, al establecer perfiles negativos o perfiles sintéticos electrónicos (como también se les llama) de los mismos, mediante la interrelación de los datos proporcionados (Ejemplo: las operaciones crediticias y el movimiento de las cuentas corrientes y de ahorros) o *inferential relational retrial.* De esta forma se afecta lo que se ha dado en llamar la identidad informática. Además esta información nominativa puede ser alimentada con datos falsos o erróneos con lo cual se ocasiona una alteración de la identidad del cliente.

La mencionada identidad informática (para otros personalidad sintética) puede formarse mediante técnicas tales como: el *mail cover*, o sea la reconstrucción de las comunicaciones existentes a través del registro computarizado de los nombres y apellidos de los remitentes y destinatarios de la correspondencia postal; la difusión de los test sicológicos de aptitud e inteligencia requeridos entre otras cosas para optar por posiciones laborales, y en los cuales se hacen preguntas diversas sobre la vida privada de las personas; la difusión de los informes de las agencias de credit report o centrales

de riesgo, que contienen datos sobre los modos de vida, solvencia y hábitos de los solicitantes de crédito (Parellada, 1990: 179 a 181).

Hay quienes como Bustamante Alsina (Bustamante, 1993a: 639), han estimado que los ilícitos informáticos sólo importan por la violación de la información nominativa y sólo la de las personas naturales. Sin embargo, como hemos visto ello no es así, ya que los ilícitos también pueden afectar a las personas jurídicas, así como involucrar información financiera y de otra índole.

Este bien jurídico va a resultar afectado casi que por las mismas causas que el bien jurídico honor. Sin embargo, en este caso lo importante es que el sistema informático de los bancos es susceptible de cambiar la verdadera identidad de las personas cuando se incurre en errores. Así un buen cliente puede ser para el sistema un mal cliente y viceversa, pero mientras se aclara la confusión de identidades creada por el mal uso del sistema, la persona afectada sufrirá los efectos del daño causado, daño en principio restringido a la esfera moral, pero que al igual que en el caso del honor, al ser susceptible de afectar intereses patrimoniales de la persona, por la pérdida de acceso a ciertos servicios bancarios, puede llevar en definitiva a daños patrimoniales indirectos. Así es evidente la existencia de un paralelismo entre el honor y la identidad como bienes jurídicos que pueden ser afectados por los riesgos de la informática, con la única diferencia de que estamos frente a dos bienes jurídicos que aunque parecidos, presentan las diferencias conceptuales que se infiere de sus definiciones.

II. Supuestos de responsabilidad del banco.

Al referirnos a los supuestos de responsabilidad de los bancos frente a sus clientes, queremos dar a conocer en forma genérica y no casuística, los principales casos en los cuales los bancos incurren en responsabilidad civil, sea esta contractual o extracontractual, fundamentalmente por la inobservancia de sus deberes y obligaciones para con los clientes. Como ya lo mencionamos, al no estar penalizadas en nuestro país las conductas conocidas en la Doctrina y el derecho comparado como delitos informáticos o lo que es lo mismo, hechos ilícitos informáticos, tales conductas para los efectos de nuestra legislación, deben caer dentro del marco de las conductas civilmente responsables, sin que tal responsabilidad devenga precisamente de la comisión de un delito, como se concibe el concepto en el ámbito penal, sino más bien de dolo o culpa civil, es decir de un ilícito civil.

Los flujos de datos en la banca representan instrucciones que, en últimas, trasladan activos. La velocidad con la cual los activos pueden transferirse al utilizar los sistemas de pagos y de intercambio de mensajes electrónicos, dificulta la tarea de control interno. Los fraudes cometidos no sólo le causan a la institución una pérdida financiera directa (daño patrimonial) sino que cuando salen a la luz pública, deterioran la confianza en la institución y en el sistema bancario en general (daño moral y patrimonial indirecto). La amplia variedad de formas en la que se puede lograr acceso a los registros del computador, crea muchas posibilidades de fraude.

Estos supuestos responsables de la informática bancaria y principalmente en lo que a los bancos se refiere, se derivan ya sea de la inadecuada manipulación de la información, de su difusión no justificada o de su falsedad (Parellada, 1990: 229). Por ello tales supuestos podrían clasificarse, a nuestro juicio, en tres grandes áreas, a saber:

1. La pérdida total o parcial de la información almacenada y que guarda relación con los clientes del banco, independientemente de su naturaleza personal o patrimonial.

2. La alteración o distorsión de la información sobre los clientes.
3. El acceso, la sustracción y posible divulgación de dicha información por terceros no autorizados por la Ley, por el propio cliente o en razón de acuerdos contractuales entre el banco y sus clientes.

Veamos en que consisten estos supuestos, en función de las tres áreas identificadas anteriormente.

A. Pérdida total o parcial de la información.

La pérdida total o parcial de la información de los clientes de un banco se puede dar ya sea por problemas de carácter meramente técnico, fundamentados en desperfectos del *hardware* o del *software*. En estos casos entra en juego el adecuado mantenimiento que el banco les brinde a estos esenciales componentes del sistema informático, de tal forma que si los deberes técnicos que el banco debe asumir, según lo previsto en el capítulo anterior, no son observados de la forma profesional con que deben asumirse, el banco incurrirá en responsabilidad contractual frente a sus clientes, al no poder cumplir con sus obligaciones de rendimiento de cuentas y de confidencialidad o reserva de la información. Sin embargo esta pérdida también puede ocasionarse en razón de un caso fortuito, o sea por razones involuntarias para los responsables de la entidad bancaria, en cuyos casos, el banco sólo será responsable, en nuestro concepto, si la pérdida es el resultado de la falta de adopción de las medidas de prevención que bajo la denominación de planes de contingencia debe llevar adelante la entidad, según lo señalado en el capítulo anterior y las cuales pueden impedir o al menos disminuir los efectos negativos en el sistema informático.

Pero también pueden ocasionarse las pérdidas en razón del acceso no autorizado al sistema por parte de terceros, de clientes de la entidad bancaria e inclusive de empleados del propio banco que provocan con su actuar, la destrucción o inutilización del soporte lógico, o sea de los datos y/o programas contenidos en un computador. Tal modalidad se presenta sobre todo por la introducción en el computador de los llamados virus informáticos, cuando estos provocan la destrucción de toda o parte de los programas y de los bancos de datos del sistema. En este último caso, la responsabilidad para el banco será igualmente contractual por la imposibilidad de rendir cuentas a sus clientes sobre sus asuntos en el banco y por el hecho de no haber incorporando al sistema los programas de antivirus y de seguridad necesarios para evitar estos insucesos, lo cual forma parte de las responsabilidades de todo buen profesional de la informática y con mucho más razón de la informática bancaria.

Generalmente la pérdida de información sólo puede implicar beneficios para quienes pretenden destruir la fuente de pruebas de sus obligaciones para con el banco, pues tratándose de las operaciones pasivas sólo la intensión de causar un daño a la Institución puede ser motivaste de la acción delictiva.

B. Alteración de la información sobre los clientes.

Otro de los supuestos de responsabilidad para el banco lo es la alteración que puede recaer sobre la información almacenada en los sistemas informáticos de los bancos. Esta alteración es causada fundamentalmente a través del acceso no autorizado al sistema por parte de terceros o por los propios empleados del banco con fines ilícitos,

sin descontar el posible acceso de clientes del banco quienes resultan motivados para buscar que los datos sobre sus asuntos o sobre los asuntos de terceros no se correspondan con la realidad, derivando en fraude informático, el cual ha sido definido como: "....la incorrecta modificación del resultado de un proceso automatizado de datos, mediante la alteración de aquellos que se introducen o están ya contenidos en el ordenador, en cualquiera de las fases de su procesamiento o tratamiento informático, siempre que sea con ánimo de lucro y en perjuicio de un tercero" (Jijena, 1992: 106).

En todo caso las alteraciones de los datos y los programas se producen en la captación de datos (*input*), en el procesamiento de éstos o en su salida (*output*).

Respecto del acceso con fines ilícitos al sistema, éste puede incluir:

1. La introducción al sistema de computación de transacciones no autorizadas.

2. La introducción de cambios no autorizados durante el desarrollo o mantenimiento de rutina, los cuales pueden hacer que el programa genere automáticamente transacciones fraudulentas, que ignoren el control de determinadas cuentas o que supriman los requisitos de transacciones específicas.

3. La existencia de programas especiales para hacer cambios no autorizados en los registros del computador en forma tal que se desvíen del control normal y de los servicios de rastreo de auditoría contenidos en los sistemas de informática.

4. El retiro físico de los activos del computador de una instalación de informática, modificados en cualquier otro lugar mediante la inserción de transacciones o saldos fraudulentos y devueltos para el procesamiento.

5. La intercepción y modificación de transacciones en forma fraudulenta mientras se transmiten a través de redes de comunicaciones.

Las nuevas formas de pagos que permiten que éstos sean iniciados por terceros mediante la utilización de equipos electrónicos pueden incrementar la posibilidad de la comisión de alguno de estos tipos de fraudes a través del acceso no autorizado a las redes de telecomunicaciones (Superintendencia, 1990: 38).

También puede realizarse la alteración de la información, ya sea antes o durante la entrada al computador, en lo que se conoce como las modificaciones de los documentos fuente. Estas modificaciones pueden consistir en: la omisión del ingreso de ciertas informaciones, la alteración de su contenido, la inclusión de datos no autorizados y el procesamiento duplicado de datos. Esto lo puede realizar cualquier persona que tenga acceso al proceso de crear, registrar, transportar, codificar, examinar o convertir la información que entra al computador. Tales alteraciones se realizan también mediante la introducción de diversos virus, que no son más que programas creados con la finalidad de alterar o destruir (como señalamos anteriormente) la información almacenada en el computador o, dicho en otras palabras: "programas de cómputo que alteran sistemas de tratamiento automatizado de información y sobre los cuales no existiría un mayor control" (Jijena, 1992: 127).

La producción de estos programas o antiprogramas, como deberían ser llamados, fue la fórmula originalmente utilizada para dar protección a los programas de las grandes compañías de *software* de los Estados Unidos. El mecanismos consistía en generar un código protector que introducido a un programa, actuaba de manera diferida cuando se producían copias no autorizadas del programa realizado.

Los virus pueden clasificarse así:

1. Benignos, cuando sólo se limitan a entregar ciertos mensajes, sin alterar sustancialmente el disco del computador.

2. Malignos, los cuales son aquellos que sí causan daños como borrar archivos y en general, evitar el normal funcionamiento de los programas y del equipo.

3. Envasados o de origen, o sea los que son introducidos al programas del computador con el fin de evitar copias no autorizadas.

4. Introducidos o direccionados, cuando se incorporan al programa del computador por terceros distintos de sus productores.

5. Los de acción inmediata, cuando actúan tan pronto son introducidos al programa.

6. Los de acción retarda, cuando su activación se produce tiempo luego de ser instalado.

Una de las principales características de los virus es su capacidad para infectar o dañar programas sin que el usuario del computador pueda inicialmente enterarse y también su efecto multiplicador, es decir su facilidad para reproducirse de computador en computador como si se tratara de una verdadera epidemia. Y es que "cualquier atentado que significase desviar el correcto desempeño de la máquina, con la finalidad de producir un perjuicio que redunde en un beneficio material o moral, para sí o para otro" (Ibidem: 94), es a juicio de Jijena Leiva, un ilícito, en nuestro caso un ilícito civil. Y estos incluye los casos en que los virus se utilizan como una supuesta protección de los derechos intelectuales sobre un *software* determinado, para que quien utilice el *software* sin autorización sufra las consecuencias dañosas de un subprograma que destruye el programa ilícitamente obtenido, pero que también puede causar otros daños a la parte lógica del sistema. Lo cierto es que no puede combartirse un daño con otro daño, máxime cuando se trata de obtener una supuesta justicia privada.

Ahora bien, entre los principales virus podemos mencionar:

1. El Caballo de Troya: Este programa es legítimo, pero contiene módulos u otros programas usualmente maliciosos (Carreño, 1990 : 147) Mediante el mismo se colocan instrucciones adicionales en un programa para que además de las funciones propias, efectúe una función no autorizada. Por ejemplo: un juego de computador que formatea (borra la información) del disco duro del computador mientras se juega; acreditar la cuenta bancaria o acreditar un salario en la cuenta designada por el cliente. Se plantea también un ejemplo, en el cual, dentro del sistema de un banco se introduce una modificación al programa de cuentas corrientes, para que siempre que sea consultado el saldo de alguna cuenta determinada, el mismo sea multiplicado por mil, diez mil, cien mil, etc. El Caballo de Troya es activado siempre que se corre el programa.

2. Técnicas de Salami: Las cuales se utilizan sobre todo en instituciones donde se mueve dinero en grandes cantidades (incluyendo la transferencia electrónica de fondos). La misma consiste en el robo de pequeñas cantidades a un gran número de registros. En este caso el acto delictivo se repite automáticamente y de forma indefinida, sin intervención del defraudador. Un ejemplo de esta práctica consiste en el redondeo de una cuenta bancaria y el acreditamiento de los montos resultantes en una cuenta designada por el delincuente.

> Se cita el caso de un empleado bancario, en los Estados Unidos, que redondeaba centavos en los cálculos de saldos de cuentas corrientes, transfiriendo a una cuenta personal, tres o cuatro centavos por transacción. En un período de cinco a seis años dicho empleado amaso una fortuna de varios millones de dólares. Sin embargo, el mismo fue descubierto ante el reclamo de un cliente a cuyo saldo le faltaban tres centavos.

3. Bombas Lógicas: Se implementa en el programa una condición o estado específico para hacer el fraude. Hasta tanto tal condición o estado no se cumpla el

programa trabaja normalmente. Por ejemplo puede instruirse la destrucción de todos los registros financieros en un fecha dada. En todo caso esta será una forma del denominado sabotaje informático.

Tanto las bombas lógicas como los caballos de Troya afectan sólo a los usuarios de computadores personales (PC) y se limitan a los programas que los contienen y a los sistemas en que corren. Son en general programas que se activan en momentos específicos o bajo ciertas condiciones y que tienen por finalidad la destrucción de la información o la alteración del funcionamiento del sistema.

4. Escobitas: mediante estos programas se busca obtener información dejada en el computador o en sus dispositivos.

5. Gusanos: son programas diseñados para escudriñar en la memoria del computador, los discos o ambos, de tal forma que se alteren todos los datos que encuentren.

En algunos casos los virus son capaces de propagarse a otros programas en el mismo microprocesador, a otros microprocesadores e inclusive afectar las copias de seguridad.

Como los principales síntomas de la existencia de los virus podemos mencionar: la mayor lentitud en la ejecución de los programas, el bloqueo del funcionamiento de la pantalla o la aparición de signos extraños en la misma y la desaparición de informaciones almacenadas en el disco duro.

Otros virus más sofisticados y de nombres extravagantes son:

1. El denominado virus Jerusalén o virus de la Universidad Hebrea, el cual se copia a si mismo, infectando los archivos ejecutables. Este actúa de tal forma que cuando un archivo infectado es ejecutado por el sistema operativo, este virus instala un programa llamado *Terminate and Stay Resident* en la memoria *RAM* del ordenador y

aunque no daña los archivos de datos de un disco duro, contamina el computador de tal forma que la única manera de eliminarlo es formateando (borrando la información) la unidad. Este virus provoca que el trabajo del computador se haga más lento, además duplica y hace crecer los archivos del computador, con lo cual éstos ocupan más memoria y completan su capacidad de almacenamiento.

2. El virus denominado paquistaní, el cual fue elaborado para supuestamente proteger las copias genuinas de *software*, pero que igualmente inutiliza la información contenida en el sistema.

3. El llamado *data crain*, o sea un virus de origen desconocido que opera con el encendido de la computadora los días martes 13. Este virus destruye las memorias de las máquinas.

4. A los anteriores virus podemos añadir la modalidad denominada puertas con trampas o *trap doors*. Esta consiste en el hecho de que en los sistemas informáticos siempre se da la existencia de puntos débiles que permiten acceder al mismo evadiendo los controles establecidos. En estos casos, los actores del ilícito se aprovechan de las interrupciones en la lógica de los programas, las cuales son establecidas a propósito por los programadores para la revisión del mismo en la etapa de desarrollo, para los efectos de depuración, y que no necesariamente desaparecen cuando se llega al proceso o etapa de producción. Estas puertas falsas son descubiertas por los delincuentes para introducirse al sistema e incurrir en el actuar doloso.

4. El *superzapping* (denominado así por el programa superzap o programa de acceso universal que permite ingresar a un computador evadiendo sus controles), el cual comienza con la utilización no autorizada de programas utilitarios o de uso universal (*software* de aplicación), a raíz de la copia que de los mismos se hace, no pagando en consecuencia los derechos, licencias de uso o royalties. Mediante tales

programas se copian, borran, usan o alteran datos almacenados en un soporte magnético, sin que quede constancia de la modificación.

Lo cierto es que ante la imposibilidad de aislar o eliminar los virus, la única alternativa posible resultan ser los llamados programas antivirus o vacuna, a los cuales ya hicimos referencia en el capítulo anterior (Supra, pág. 122).

Todos estos virus pueden también entrar a las computadoras de los clientes de los bancos, si tomamos en cuenta que con el desarrollo de la llamada banca hogareña o *home banking*, ya los clientes pueden desde terminales en sus casas o desde sus propias computadoras personales, acceder a sus registros en el banco. En este caso, si el sistema bancario esta contaminado con un virus, el mismo puede afectar gravemente la memoria de la computadora de un cliente.

En cuanto a los accesos no autorizados a los archivos de información en el computador, al equipo o a cualquiera de sus dispositivos, se ha establecido una gradación de los niveles de seguridad del computador y en función de las habilidades técnicas que se requieren para eludir los controles que impiden dicho acceso, así tenemos:

Nivel 1 : No se requieren conocimientos técnicos para el acceso.

Fraudes del usuario, fraudes en el proceso de entrada, salida, búsqueda de listados, suplantación, adulteración de documentos fuente y robo de archivos

Nivel 2: Se requieren conocimientos técnicos moderados para el acceso.

Manipulación de programas, búsqueda en línea, examen de discos scratch, técnica del salami.

Nivel 3: Se requieren conocimientos técnicos avanzados para el acceso.

Fraudes en sistema operacional, penetración de sistemas TP, bombas lógicas, intercepción, superzaping (Carreño, 1990: 131).

Los objetivos que se buscan con estas alteraciones pasan por el robo de los activos, es decir el débito a las cuentas de los clientes; la ocultación de las deudas u obligaciones para con el banco, la manipulación de ingresos y la manipulación de egresos (Carreño, 1990:129).

C. El acceso, la sustracción y la divulgación de dicha información por terceros no autorizados.

Bajo este supuesto se considera una acción que genera responsabilidad por el simple hecho en virtud del cual, una persona no autorizada ni contractual, ni legalmente (en el ámbito informático denominados *hackers*) accesa la memoria del computador y toma conocimiento de la información confidencial sobre un cliente de un banco o procede a copiar dicha información, ya sea mediante programas copiadores o por otros medios, o la sustracción de la misma -generalmente mediante redes telemáticas[4] - con el fin de darla a conocer a terceros o para otros fines que lesionan la intimidad de los clientes afectados y más específicamente, violentando las disposiciones sobre secreto o reserva bancaria que son característica fundamental de la actividad. En este caso el banco asumiría una responsabilidad si se comprueba que incumplió sus obligaciones técnicas de seguridad sobre el sistema informático, que reclama la disciplina informática, o sea si se comprueba su culpa. De lo

---

4 El término telemática fue adoptado en Francia con el fin de designar el procedimiento de elaboración a distancia de las informaciones y el movimiento de circulación automática de los datos informativos, el cual se produce en razón del diálogo con las computadoras electrónicas, utilizando con tales objetivos, terminales inteligentes, o sea que reciben y transmiten.

contrario, es decir, no comprobándose su culpa, el mismo podría excusarse sobre la base de que el hecho de un tercero originó el daño.

Debe tenerse como principio básico, que todo acceso al computador se presume ilegítimo salvo que medie una causa de justificación. Como causas de justificación hay quienes señalan que la existencia de un interés superior sería suficiente, mientras que otros manifiestan que se requiere una ley que califique el interés como superior.

En el caso de los *hackers* (escavadores subterráneos) éstos penetran a los sistemas teniendo previo conocimiento del número telefónico que les permite conectarse con la entidad en la que se ubica la computadora, luego descubren el número o símbolo que les permite acceder a la sesión de trabajo y finalmente la clase de acceso a los archivos reservados.

En estos casos, también denominados de espionaje informático, el banco puede incurrir en responsabilidad, toda vez que es una obligación del mismo, como ya señalamos, el asegurarse de que su equipo informático esta dotado de los sistemas de seguridad necesarios para evitar los mencionados ilícitos, de tal manera que la inexistencia o ineficacia de dichos sistemas resulta atribuible en todo a la entidad bancaria, que ha optado por el uso de un sistema informático asumiendo no sólo los beneficios del mismo sino también sus riesgos. Además, el banco asume una responsabilidad profesional en estos casos, no sólo de carácter bancario sino también en el ámbito informático, sea esta de carácter directo, cuando el mismo opera por si mismo el sistema, o de carácter indirecto, cuando contrata el servicio con terceros, presuponiéndose que el banco o sus contratistas tienen el conocimiento y la habilidad profesional para el adecuado manejo del sistema informático seleccionado. En abono de lo anterior, la Doctrina señala que este ilícito se ve favorecido por la desprotección

material y logística, sea técnica o administrativa de las bases de datos informatizadas, así como por el hecho de que dicha información, en razón de la tecnología que lo hace posible, se concentra en espacios reducidos y rápidamente accesibles (Iijena, 1992: 106).

CONCLUSIONES Y RECOMENDACIONES

I. CONCLUSIONES.

1. La responsabilidad civil es aquella que surge como resultado de una conducta positiva o negativa que ocasiona un daño y que contraviene el ordenamiento jurídico, ocasionando que el autor de tal conducta deba cumplir una sanción o indemnizar al ofendido, en ambos casos según las previsiones legales aplicables.

2. La responsabilidad civil se clasifica en contractual, o sea aquella que presupone la existencia de un vínculo jurídico entre el autor del hecho dañoso y la víctima del mismo; y, extracontractual cuando no existe tal vínculo.

3. La responsabilidad contractual y extracontractual presentan diferencias en cuanto a su origen, la gradación de la culpa, la solidaridad, la carga de la prueba, la extensión del resarcimiento, la mora, la atenuación de la responsabilidad y la prescripción.

4. Son elementos comunes de la responsabilidad civil: la antijuridicidad, el daño, la relación de causalidad entre el daño y el hecho y los factores de imputabilidad o atribución legal de la responsabilidad.

5. Los factores de imputabilidad o atribución legal, pueden ser subjetivos, tales como: el dolo y la culpa; u, objetivos tales como el riesgo, la garantía, la equidad, el abuso del derecho y el exceso de la normal tolerancia, todos los cuales prescinden del factor culpa.

6. En la Legislación panameña y el derecho comparado son factores preponderantes los subjetivos.

7. Existe un concepto de responsabilidad profesional en el ámbito doctrinal y del derecho comparado, el cual resulta atribuible a aquellos que ejercen una profesión, al faltar a los deberes que su disciplina o ciencia le imponen, o sea al estereotipo del buen profesional, surgiendo así la culpa profesional.

8. Las obligaciones de los profesionales pueden ser de medios o de resultados, según sea que se garantice o no el resultado de la labor profesional.

9. La relación entre el profesional y sus clientes será siempre contractual, pues la misma se fundamenta en un contrato previo, lo cual no implica que pueda contraer igualmente una responsabilidad extracontractual con terceros, en virtud de ilícitos civiles o penales.

10. Los bancos son susceptibles de incurrir en responsabilidad civil, la cual será generalmente contractual y profesional.

11. Existe antetodo en la jurisprudencia extranjera, una multiplicidad de casos relacionados con la responsabilidad civil en que han incurrido los bancos en la realización de contratos que incluyen operaciones activas, pasivas o neutras.

12. A pesar de que la mayor parte de las obligaciones que asumen los bancos son de resultado, también pueden en algunas ocasiones contraer obligaciones de medios.

13. Cuando el banco actúa a través de sus organismos directivos, puede incurrir en una responsabilidad directa o por el hecho propio; si el daño lo causan sus empleados esta responsabilidad será indirecta o por el hecho ajeno.

14. El actuar del banco puede implicar la lesión de diversos bienes e intereses jurídicos protegidos, sean estos de naturaleza tangible o intangible.

15. La actividad bancaria es aquella que realiza la empresa mercantil que como parte de un sistema presta un servicio público de forma masiva y a través de la fórmula de la intermediación financiera, asumiendo los riesgos que resulten y con una cuidadosa reserva de la información que obtengan de sus clientes frente a terceros.

16. Nuestra legislación define la actividad bancaria no con base en sus principales elementos, tal y como lo hace la doctrina, sino sobre la base de la intermediación financiera. Así lo dispone el literal b del artículo 2 del Decreto de Gabinete 238 de 2 de julio de 1970.

17. La Ley 29 de 1 de febrero de 1996, por la cual se dictan normas sobre la defensa de la competencia y se adoptan otras medidas, resulta aplicable a la actividad de los bancos, principalmente en lo que atañe a la relación contractual con sus clientes, de la cual deriva el hecho de que los bancos deban asumir múltiples obligaciones en previsión de la nulidad de los instrumentos jurídicos que originan los derechos y obligaciones entre éstos y sus clientes.

18. El hecho informático es aquel relativo al tratamiento racional, automático y sistemático de la información por medios electrónicos. El hecho informático bancario será entonces el desarrollado por las entidades bancarias, teniendo por objeto la información propia y principalmente, la información tanto personal como financiera de sus clientes.

19. La información masiva que recogen los bancos y que almacenan en la memoria de sus computadores pasa a denominarse banco de datos, los cuales son organizados e interrelacionados.

20. Existe un incipiente derecho informático cuyo objeto es la regulación de los instrumentos informáticos, la protección de la intimidad, los contratos informáticos, los

delitos informáticos, la responsabilidad civil por daños emergentes de la informática y el derecho procesal informático.

21. La finalidad de la informática bancaria es la utilización de las facilidades tecnológicas para conseguir la integración de una memoria capaz de conservar y restituir datos de forma constante, con capacidad de combinar automáticamente datos existentes para crear nuevos datos y la capacidad de operar a una velocidad mayor que los métodos tradicionales, obteniendo de esta forma un sistema efectivo para el manejo y utilización práctica de la información bancaria y por ende una mayor eficacia de la empresa bancaria.

22. Una de las expresiones más palpables del uso de la informática aplicada a las operaciones bancarias, la tenemos en las denominadas transferencias electrónicas de fondos (TEF), las cuales han permitido la aparición de los servicios de cajeros automáticos, puntos de venta, banca hogareña, *clearing* bancario, banca virtual y la tarjeta inteligente, entre otras.

23. La transferencia electrónica de fondos no es más que aquella herramienta de la tecnología que permite por medios electrónicos, el traspaso de fondos entre cuentas, de tal forma que se efectúen pagos sin desplazamiento de dinero.

24. Las transferencias electrónicas de fondos pueden clasificarse en cuatro formas, según las cuentas involucradas, a saber: transferencias entre cuentas de un cliente, en un mismo banco; transferencias entre cuentas de diferentes clientes en un mismo banco; transferencias del mismo cliente en distintos bancos; y, transferencias entre cuentas de distintos clientes en distintos bancos.

25. Las transferencias electrónicas de fondos tienen tres consecuencias, a saber: la eliminación del papel en las relaciones entre el banco y sus clientes; la prestación de

servicios bancarios fuera del área de las oficinas bancarias; el traslado al banco de una serie de gestiones y el aumento de su responsabilidad civil frente a sus clientes.

26. Existen megaredes electrónicas de comunicaciones interbancarias de carácter generalmente privado, que procesan órdenes de pago y otros datos diversos en formatos predeterminados.

27. El uso de la informática no sólo resulta de aplicación práctica a través de las transferencias electrónicas de fondos, sino también se extiende a casi todas las operaciones bancarias.

28. El hecho ilícito informático se caracteriza por que el banco como consecuencia del uso de la tecnología informática, causa un daño a sus clientes, al propio banco o terceros. La posibilidad de que se ocasionen estos daños son riesgos que los bancos deben asumir en muchos casos.

29. Los riesgos mencionados pueden ser de naturaleza diversa. Así podemos mencionar los riesgos financieros, operacionales, administrativos, relacionados con los medios, con errores e intencionales.

30. La informática bancaria se ha desarrollado en Panamá desde fines de los años sesenta, sin embargo es en los años setenta, cuando los primeros bancos empiezan a desarrollar programas de innovación tecnológica hasta alcanzar en la actualidad un cien por cien de los mismos, los cuales han automatizado la casi totalidad de sus operaciones.

31. La naturaleza jurídica de la responsabilidad de los bancos frente al hecho informático bancario puede ser de carácter contractual o extracontractual.

32. La responsabilidad será contractual cuando la obligación de reparar el daño ocasionado, resulte precedido por un contrato celebrado entre el banco y la persona lesionada.

33. La responsabilidad del banco derivada de la relación jurídica perfeccionada en un contrato, generará principalmente obligaciones de resultado, de tal forma que ante un daño el banco sólo podrá eximirse probando la culpa de un tercero por quien no deba responder o por caso fortuito extraño al riesgo del sistema.

34. La responsabilidad del banco en materia informática será también profesional, pues el mismo si bien no es un profesional de la informática como disciplina general, si lo debe ser de la informática bancaria, y en tal sentido, se le aplicará la regla *probatio incumbit facilius probandi,* según la cual aquel que se encuentre en mejores condiciones para demostrar el origen de un daño, es quien debe ser gravado con la carga de la prueba.

35. Además de los contratos, las obligaciones de los bancos en el tema que nos ocupa, también derivará de las leyes que regulen la materia informática.

36. Las cláusulas de exoneración, liberación o limitación de responsabilidad en materia informática, no son reconocidas tratándose de dolo o culpa grave y máxime cuando la Ley 29 de 1996, las considera absolutamente nulas.

37. La doctrina y la jurisprudencia extranjera, se pronuncia en defensa de la parte más débil en la relación banco-cliente y propugnan por la aplicación en materia bancaria, de la responsabilidad objetiva y por el riesgo creado, de tal forma que la responsabilidad deba recaer siempre en la empresa que busca y obtiene un provecho económico creando un riesgo, más no en el cliente.

38. Gran parte de la doctrina reconoce a la informática como una cosa o actividad peligrosa que amerita la aplicación de la teoría del riesgo, principalmente en lo que atañe a la denominada gestión de *banco de datos.*

39. Si la responsabilidad del banco se tiene por contractual objetiva, sus obligaciones son en todo caso de seguridad y por ende de resultado.

40. La responsabilidad de los bancos en materia informática también puede ser extracontractual, cuando la relación de éstos con terceros no resulta precedida de un contrato. Las obligaciones de los bancos en este sentido surgirán principalmente de la revelación de datos incorrectos a dichos terceros.

41. También habrá responsabilidad extracontractual para los bancos cuando se incurra en el denominado delito informático, o sea el instrumentado mediante el uso de computadoras.

42. La Legislación penal vigente en Panamá carece de los tipos penales que permitan con certeza afirmar que en nuestro país se castiga, lo que en otros se conoce como delito informático.

43. En el derecho comparado encontramos legislaciones que regulan las relaciones jurídicas derivadas de la informática únicamente en el ámbito civil, principalmente con relación a las informaciones nominativas, o sea aquellas que tienen una relación más directa con el bien jurídico intimidad.

44. Igualmente, parte de la doctrina se inclina por la regulación de los hechos ilícitos informáticos únicamente en el ámbito civil, aunque las modernas tendencias sugieren que la información es un bien jurídico susceptible de tutela tanto en el ámbito civil como penal.

45. La responsabilidad civil extracontractual del banco puede ser la que corresponda a su calidad de dueño, guardián o principal del equipo de cómputo, incluyendo *hardware* y *software*.

46. El banco puede ser responsable por los ilícitos informáticos de sus empleados cuando los mismos consistan en fraudes tales como el acceso a registros de cuentas o al equipo, más no así cuando el fraude sea el resultado de los conocimientos que el empleado haya adquirido en el curso de su trabajo.

47. En los Estados Unidos se ha pretendido resolver el problema del resarcimiento dimanante de las acciones legales en materia informática mediante el uso de los llamados *torts theories.*

48. En cuanto a la naturaleza de la responsabilidad de los bancos tratándose de la gestión de bancos de datos, la doctrina y parte del derecho comparado se inclina por asignarle un carácter objetivo, a través de leyes de datos y sobre la base de las obligaciones de garantía que se derivan de dicha actividad.

49. En Panamá, careciéndose de leyes de datos, sólo resulta viable la aplicación de las disposiciones genéricas sobre responsabilidad civil de carácter subjetivo.

50. La responsabilidad derivada de la informática puede considerarse como una responsabilidad por cosa o actividad peligrosa, cuando un programa se destina a actividades que puedan importar peligro para el usuario y terceros en forma difusa.

51. Existe una posición ecléctica que promueve el criterio de que la responsabilidad puede ser objetiva o subjetiva, dependiendo de si la misma proviene de dolo o culpa del operador de la computadora o del vicio o riesgo.

52. El carácter contractual de la obligación se traduce en el hecho de que el gestor del *banco de datos* siempre tiene un deber genérico de cuidado sobre la información, por tal hecho debería irrogársele una responsabilidad objetiva, pues en caso contrario la víctima de una violación de la intimidad vería muy difícil probar el ilícito y solicitar la reparación del daño.

53. La afirmación anterior viene reforzada con el argumento de que en materia de violaciones al derecho a la intimidad, la intromisión debe ser arbitraria y no necesariamente dolosa o culposa, para que se admita la reparación del daño. Y es arbitraria la intromisión cuando se violan los principios fundamentales consagrados en las leyes de datos.

54. En el plano extracontractual, la gestión de bancos de datos puede ocasionar daños patrimoniales o morales.

55. Si la responsabilidad del banco en materia informática es objetiva, éste solo podrá liberarse probando la culpa de la víctima, de un tercero por el cual no debe responder o por caso fortuito o fuerza mayor ajena a la cosa.

56. Si la responsabilidad del banco en materia informática es subjetiva, la víctima debe probar que el daño es el resultado de la culpa o el dolo del banco.

57. Si el computador es operado por un hombre, la responsabilidad podría reputarse subjetiva; si es operado en forma automática, la responsabilidad podría ser objetiva.

58. Los daños que el banco causa a sus clientes por revelar a personas no autorizadas información electrónicamente almacenada o por no dar cuenta de la misma a sus clientes, hacen surgir una obligación contractual de reparación para con el cliente, siendo también actos antijurídicos.

59. También son actos antijurídicos, aquellos mediante los cuales el banco afecta negativamente a terceros, en razón del uso de la tecnología informática.

60. El factor daño se produce por la lesión que el banco causa, cuando como resultado del procesamiento electrónico de la información se lesiona el patrimonio, la intimidad, el secreto bancarios, la identidad y aun el honor de sus clientes, o se les priva del disfrute de los derechos o la expectativa lícita a continuar disfrutando de los derechos sobre bienes jurídicos protegidos.

61. El daño informático comprende el tratamiento ilícito de la información nominativa, pero también los datos no nominativos, antetodo cuando éstos son deficientes o erróneos.

62. Para los efectos de la responsabilidad civil, se analizan los daños provenientes de la información electrónicamente tratada, ya sea en su ingreso o en su salida, y no de los daños causados por el *hardware* o el *software* como cosas en sí. Sin embargo, el banco deberá asumir responsabilidad para con su cliente en razón de un *software* deficiente cuando medie un contrato entre ellos, pues de modo contrario no habría responsabilidad, al menos en nuestra legislación, en vista de la inexistencia de responsabilidad indirecta por el hecho del software como cosa.

63. Para que surja responsabilidad, debe haber un nexo causal entre el actuar del banco como controlador de un sistema informático y el daño que el uso por parte del banco de dicho sistema causen al patrimonio, la intimidad, el secreto, el honor o identidad personal del cliente.

64. La relación de causalidad puede interrumpirse si se prueba que el daño fue el resultado del actuar del propio cliente o de caso fortuito o fuerza mayor.

65. Para que, conforme a nuestra legislación, el banco asuma una responsabilidad, debe probarse que el mismo incurrió en dolo o culpa en el procesamiento y almacenamiento de la información.

66. Los bancos tienen obligaciones de carácter legal frente a sus clientes en razón del hecho informático, entre las cuales destacan: la obligación de rendir cuentas y la obligación de reserva.

67. Los bancos tienen también obligaciones de carácter técnico cuyo incumplimiento puede derivar en daños para con sus clientes. Esto principalmente porque el banco asume una responsabilidad profesional en todos los ámbitos de su actividad.

68. Como corolario a lo anterior, el banco asume la responsabilidad de que el sistema informático funcione sin causar ningún daño a sus clientes o terceros,

asumiendo las causas perjudiciales que ocasionan las fallas en el sistema, como resultado de un manejo técnicamente deficiente o por la omisión en el seguimiento de prácticas preventivas o correctivas de los bienes que componen dicho sistema.

69. Existen legislaciones en el derecho comparado y a nivel del derecho internacional, que regulan el flujo de datos transfrontera o *transborder data flow,* principalmente tratándose de información sensible que es transmitida a países que carecen de una legislación que tutele el derecho a la intimidad y sobretodo de sus datos personales. Estas legislaciones se fundamentan en el principio de reciprocidad.

70. Existe una transferencia internacional de fondos, cuando la misma se realiza entre bancos ubicados en diferentes países.

71. No existen normas aplicables a las transferencias internacionales de fondos, salvo las que rigen para ciertas redes privadas.

72. La ley aplicable, tratándose de transferencias internacionales de fondos por medios electrónicos, resultaría ser la que corresponda al país de cumplimiento de las obligaciones, o sea el país del destino de la transferencia conforme a la doctrina y a las normas de derecho internacional privado. En caso de responsabilidad civil extracontractual, será aplicable la ley del lugar de la comisión del ilícito, conforme a lo que expresa, entre otros, el Código de Bustamante.

73. A falta de normas aplicables a las transferencias internacionales de fondos por medios electrónicos, se propone la recopilación de los usos bancarios internacionales en convenciones elaboradas por entidades internacionales especializadas, que pasen a formar la *Lex Mercatoria* en el tema.

74. El banco causa daños patrimoniales a sus clientes, al decidir utilizar la tecnología informática para el procesamiento electrónico de sus operaciones y la

información que es inherente a dichos clientes, cuando tal uso lesiona un interés relativo al patrimonio de éste.

75. Los daños patrimoniales que un banco puede irrogar a sus clientes a través del uso de la informática, se plantean principalmente mediante hechos relacionados con las trasferencias electrónicas de fondos (TEF).

76. La responsabilidad civil patrimonial por las transferencias electrónicas de fondos se encuentra reconocida y ampliamente regulada en la Legislación de los Estados Unidos de América, de la cual bien pueden extraerse principios para la elaboración de los derechos positivos de otros países en esta materia.

77. El derecho tiene el reto de regular las consecuencias jurídicas que surgen del uso de las nuevas tecnologías bancarias tales como las tarjetas inteligentes y del dinero o moneda E, las cuales surgen al propiciar las transferencias de valores por medios electrónicos y el aumento del riesgo de pérdida patrimonial para los clientes bancarios.

78. El concepto de derecho a la intimidad, a pasado de garantizar la reserva o secreto sobre la vida privada de las personas, a constituirse en garantía del control que esa persona tiene sobre la información que le concierne. Se ha pasado entonces de una libertad negativa a una libertad positiva, o lo que es lo mismo, la autodeterminación informativa.

79. En materia informática, la intimidad viene constituida por el derecho a controlar la denominada información o datos sensibles, los cuales constituyen el ámbito íntimo y por lo tanto tutelado por la ley.

80. Las modernas tendencias consideran que los datos sensibles no deben ser calificados así por su cercanía con el concepto intimidad, sino por su utilidad y la posibilidad de su aplicación.

81. La información personal y patrimonial de los clientes, que los bancos procesan, almacenan, asocian y utilizan, esta constituida en gran medida por datos sensibles.

82. La lesión que se ocasiona al derecho a la intimidad de los clientes de un banco puede ser de carácter moral cuando se afecten intereses extrapatrimoniales, pero también de carácter patrimonial indirecto. Esto último en virtud de los perfiles financieros que los bancos elaboran sobre sus clientes y que afectan sus derechos de crédito y aún el crecimiento económico de los clientes de los bancos, sobretodo porque la misma pasa a constituir la *informática decisional.*

83. Existen derechos mínimos esenciales que en el ámbito informático deben ser reconocidos a los titulares de la información electrónicamente tratada -incluyendo los clientes de los bancos- para no lesionar su derecho a la intimidad. Estos principios han tenidos su máxima expresión en el denominado *hábeas data.*

84. El reconocimiento del derecho a la intimidad a pasado por una evolución legislativa desde el siglo XVIII hasta nuestros días, siendo reconocido en la mayor parte de las legislaciones modernas.

85. El derecho positivo de numerosos países regula la protección del derecho a la intimidad en el ámbito informático mediante la expedición de normas aplicables principalmente a los bancos de datos y el reconocimiento de los derechos fundamentales de los titulares de la información que han inspirado el surgimiento del *hábeas data.*

86. Principalmente las legislaciones adoptadas por distintos países europeos, consagran los principios que garantizan el derecho a la intimidad informática a través de la protección de los datos personales o nominativos de los titulares de los datos electrónicamente tratados.

87. En virtud de lo anterior, se define una adecuada ley de datos por la incorporación de principios tales como: la justificación social, la limitación de la recolección, la calidad o fidelidad de la información, especificación del propósito o finalidad, confidencialidad, salvaguarda de la seguridad, apertura, limitación en el tiempo, control y participación individual.

88. Existe un renovado interés por parte de los organismos internacionales en la regulación, dentro del derecho internacional, del tema de la protección a la intimidad a través de la protección de los datos personales, y sobretodo cuando los mismos pasan a formar parte del flujo de datos a través de las fronteras de distintos países.

89. Hay algunas limitaciones que repercuten en el derecho a la intimidad desde el plano de la informática bancaria, fundamentalmente cuando el interés particular que subyace en el derecho a la intimidad, debe ceder frente al interés público de conocer ciertas informaciones.

90. El interés público plantea limitaciones al derecho a la intimidad bancaria, cuando las autoridades competentes requieren conocer de ciertos datos necesarios para el cumplimiento de los fines para los cuales estas han sido instituidas.

91. También se plantean limitaciones frente a las denominadas *centrales de riesgo*, o sea los centros de información bancaria, salvo cuando la información que estas divulguen sea incorrecta. Ello es así, por cuanto se reconoce a la actividad bancaria como una actividad de interés general o público, en virtud de la cual los bancos no pueden realizar operaciones con personas sin antecedentes conocidos. Esta práctica es una defensa de los intereses institucionales, lo cual se consigue a través de las *centrales de riesgo*.

92. Los clientes no tienen derecho a impedir la divulgación de información sobre sus antecedentes financieros, sobretodo cuando son negativos, porque ello, en

términos generales, impediría el ejercicio del servicio público que prestan los bancos y porque tal información no necesariamente tiene relación con su intimidad. Sin embargo, debe prevalecer el principio de que el cliente debe haber autorizado la revelación de la información, o sea el principio de la autorización previa.

93. La información que deben revelar los bancos a través de las *centrales de riesgos* o mediante el intercambio de información interbancaria, no sólo debe ser correcta, sino que también debe ser completa, para evitar discriminaciones y distorsiones en las decisiones financieras.

94. La tutela del secreto bancario como bien jurídico protegido y su análisis por parte de la doctrina, tratándose de materia informática, resulta eclipsado, por no decir absorvido, por el reconocimiento y la evolución del bien jurídico intimidad .

95. Las distorsiones en el perfil crediticio o financiero de un cliente, como resultado de las referencias negativas suministradas por un banco, pueden dar lugar a que se lesione el honor de dicho cliente, si entendemos que este comprende el buen nombre, el valor moral y la buena reputación del mismo, así también puede lesionarse la identidad personal, para estos efectos llamada identidad informática.

96. Pueden ser supuestos de responsabilidad del banco: la pérdida total o parcial de la información de sus clientes, almacenada electrónicamente; la alteración o distorsión de dicha información; y, el acceso, la sustracción y posible divulgación de dicha información por terceros no autorizados por la ley o por los clientes.

97. La pérdida total o parcial de la información implicará para el banco una responsabilidad contractual, ocasionada por la imposibilidad de rendir cuentas a sus clientes. Este supuesto puede sobrevenir por defectos técnicos o por la introducción de los programas -o en este caso antiprogramas- denominados *virus,* contra los cuales los

bancos tienen la obligación de buscar mecanismos de prevención y defensa, sobretodo a través de planes de contingencia.

98. La alteración de la información almacenada electrónicamente en la entrada o en la salida de datos, puede ser ocasionada por empleados del banco, por terceros y aun por clientes con intensiones de cometer actos de fraude informático. Esta alteración también resulta posible mediante la introducción de los denominados *virus,* que alteran el normal funcionamiento del sistema.

99. Existen múltiples modalidades y formas de virus.

100.El acceso sin causa justificada a la memoria de un computador por personas o con fines no autorizados, así como la sustracción y la divulgación de la misma, puede generar responsabilidad para el banco cuando se comprueba su culpa, es decir cuando se comprueba que éstos no adoptaron las medidas que demandaban las obligaciones técnicas que deben asumir, y cuando los mencionados actos lesionan el bien jurídico intimidad y violentan el principio de reserva bancaria.

101.Las actividades de los llamados *hackers,* así como el espionaje informático, constituyen las principales expresiones de los supuestos mencionados en el numeral anterior.

II. RECOMENDACIONES.

Resulta un hecho cierto, que nuestra legislación requiere de una actualización acelerada con el fin de adaptarse a los tiempos modernos en los cuales la informática, como expresión máxima de las nuevas tecnologías, tiene un impacto esencial. Por tal razón, resulta imprescindible dotar a nuestro ordenamiento jurídico de los mecanismos que permitan a nuestros ciudadanos optar por fórmulas legales que les permitan proteger sus bienes e intereses jurídicos de los daños que el mal uso de estas nuevas herramientas les puedan ocasionar. Ello es así, porque si bien la tecnología moderna procura innumerables beneficios en todos los aspectos de la vida de los hombres, no es menos cierto que también los riesgos que ésta importa son imprevisibles por su acentuada vulnerabilidad a ser utilizada para fines ilícitos.

Específicamente en el ámbito bancario panameño, la protección de los clientes o consumidores de los servicios que ofrecen las entidades bancarias, a quedado reducido a un número limitado de normas de carácter administrativo en el Decreto de Gabinete 238 de 2 de julio de 1970 y en algunos acuerdos dictados por la Comisión Bancaria Nacional, así como en las disposiciones generales que conforman la legislación que sobre responsabilidad civil se encuentra recogida en el Código Civil y finalmente los artículos que dentro del Código de Comercio pasan a constituir las obligaciones de los comerciantes. Es sólo a partir de la Ley 29 de 1 de febrero de 1996, por la cual se dictan normas sobre la defensa de la competencia y se adoptan otras medidas, cuando empieza a definirse una legislación que tiende a proteger los derechos de los clientes o consumidores de servicios bancarios o financieros en general. Sin embargo cabe preguntarse, si esto sería suficiente para garantizar una adecuada protección de los bienes e intereses jurídicos de los consumidores

de servicios bancarios. Y la respuesta -en nuestro concepto- sería que no. En áreas tales como el uso de sistemas informáticos para la prestación de servicios, principalmente en lo que atañe a los bancarios, resulta necesario el establecimiento de una legislación que garantice a los consumidores e inclusive a los simples titulares de datos electrónicamente tratados, que bienes jurídicos tales como el patrimonio, la intimidad, el secreto bancario, el honor y el buen nombre no le serán lesionados. Para tales efectos, la doctrina y el derecho comparado proponen iniciativas legislativas que incluyen: una ley básica -llamada ley de datos- con principios generales que instituyen el denominado *hábeas data*, normas específicas para resolver los conflictos planteados en determinados sectores, bajo la fórmula de una responsabilidad civil preponderantemente objetiva; un órgano independiente, que en el ámbito administrativo se aboque a una supervisión estricta y difusa, así como a la reglamentación de la materia. Algunos otros países como Estados Unidos, se extienden a penalizar los ilícitos informáticos e instituyen tipos penales especiales, es decir tipifican hechos como delitos informáticos.

En materia de responsabilidad civil, se acentúa en estos casos, la tendencia por el establecimiento de supuestos de responsabilidad objetiva sobretodo a los bancos, principalmente para que las eventuales acciones de sus clientes no resulten ilusorias por la dificultad probatoria que la atribución de los daños resultantes de los hechos informáticos comúnmente ocasionan.

También se señala que lo ideal sería que la responsabilidad dimanante de tales ilícitos informáticos, se regulara única y exclusivamente en el ámbito civil.

En el caso de nuestro país, con uno de los sistemas bancarios más importantes de América Latina, no cabe duda que resulta imperativo elaborar una legislación que sin obstaculizar el normal desarrollo y crecimiento del sistema, garantice a los clientes o consumidores de los servicios bancarios, que sus bienes e intereses jurídicos no les serán

lesionados, en razón del uso que de la tecnología informática se realice, con el fin de optimar la eficiencia en la prestación de tales servicios. Estas garantías a nuestros consumidores, no sólo redundarán en beneficio de los mismos, sino también en beneficio de la credibilidad y confianza que debe mantener el sistema bancario panameño. En la actualidad, la existencia de legislaciones de datos en países europeos y de los Estados Unidos, implica para sus sistemas financieros, una ventaja comparativa frente al nuestro, lo cual resulta delicado, en momentos en que se impone el concepto de globalización.

En razón de lo anterior, si bien lo ideal sería incluir en forma expresa dentro de nuestra Constitución Política, la institución del *hábeas data,* por lo pronto lo más recomendable sería la elaboración de una legislación especial en materia informática, a la usanza de aquellas que ya empiezan a surgir en nuestro sub-continente latinoamericano.

Hacemos mención de una legislación informática de forma genérica, porque conceptuamos que elaborar una legislación específica para el sector bancario implicaría el desconocer la magnitud de la influencia de los sistemas informáticos en la prestación de otros servicios comerciales y de otra naturaleza, cuyos consumidores o simples titulares de datos tratados mediante tales sistemas también tienen derechos a la debida protección de la ley.

Así la legislación en referencia, debería tener por objetivo principal la guarda de los bienes e intereses jurídicos protegidos de todas aquellas personas naturales o jurídicas que sean titulares de cualquier dato que se encuentre o sea susceptible de encontrarse en un archivo informático, incluyendo a los clientes de los bancos; así también se establecerían las obligaciones de las personas naturales o jurídicas que utilicen o se sirvan de medios informáticos con la finalidad de recolectar, procesar o almacenar informaciones, ya sea para transmitirlas o difundirlas dentro del marco de la ley. Esto implica que esta legislación

debería hacer énfasis en las personas naturales o jurídicas que actúen como controladores o gestores de bancos de datos.

Debe contemplarse la prohibición de recolectar datos sensibles relacionados con aspectos raciales, políticos, religiosos, etc., salvo cuando sean autorizadas por sus titulares para fines que no sean contrarios a la ley y su no divulgación, salvo para fines estadísticos, siempre y cuando no sea revelado el nombre de los titulares de los mismos.

La obligación de los controladores o gestores de bancos de datos de establecer procedimientos para la corrección o actualización de las informaciones recabadas debe ser plenamente establecida.

Como parte fundamental de esta legislación debe incluirse como mínimo, la obligación de reconocer y respetar los derechos y las obligaciones dimanantes de los principios fundamentales en la protección de los titulares de datos recolectados electrónicamente. Esto implicaría que como mínimo, los controladores de bancos de datos -entre ellos los bancos- deberían obligarse a:

1. Que la captación de datos tenga un objetivo general, o sea la adecuada prestación de los servicios informáticos -entendiendo que estos constituyen un servicio público- y que sus usos sean consecuentes con la actividad propia de las entidades que los prestan.

2. Que la información debe ser recolectada por medios lícitos, o sea con conocimiento y consentimiento de los consumidores de los servicios informáticos o titulares de datos o con autorización de la ley, y siempre que se limiten a aquella que es suficiente para cumplir con la finalidad para la cual es recolectada, lo cual implica que no puede haber de por medio ni engaños, ni ocultamientos de la finalidad de la recolección. En el caso de los bancos y otras entidades financieras, éstas deben comprobar que sus clientes los han autorizado a obtener y/o verificar información sobre éstos, en los centros o bancos de datos disponibles.

3. Que los datos personales que se recolecten y almacenen serán exactos, completos y actuales, de tal forma que los mismos no den lugar a errores. Lo anterior implica que se debe reconocer el derecho de los titulares de datos a rectificar, cancelar o actualizar cualquier información inexacta o incompleta, es decir el *derecho de acceso* y de *rectificación.*

4. Que los fines u objetivos para los cuales se recolectan los datos sean especificados al momento de tal recolección, sin que se puedan utilizar para fines distintos.

En el caso de los bancos, éstos deben describir en la forma más completa posible a sus clientes, la finalidad para la cual se recogerá información personal y financiera de los mismos, y la concesión de garantías sobre el uso que se le dará a la misma.

5. Que se requiera consentimiento expreso del titular de tales datos o de la ley, para revelar cualquier información electrónicamente almacenada. En el caso de los bancos, debe establecerse que éstos quedan obligados a evidenciar que han sido autorizados por sus clientes para intercambiar información con otras entidades financieras o con centrales de riesgos o centros de información o de referencias de crédito, a fin de no menoscabar la intimidad de sus clientes y no violar la reserva o secreto bancario como elementos fundamentales de la actividad bancaria.

6. Que se adopten las medidas técnicas y de seguridad esenciales en la actividad informática, para proteger a los consumidores de servicios informáticos contra pérdidas, destrucciones o acceso no autorizado.

7. Que se garantice la transparencia de sus actos con relación a los procedimientos, desarrollo y prácticas relativas al procesamiento electrónico de datos personales. Para ello debe garantizar a los titulares de datos, la existencia, fines, usos y métodos utilizados en la operación de los registros o *bancos de datos* personales

8. Que los datos recolectados, sobretodo cuando resulten negativos, no serán almacenados en el registro o la memoria del computador, sino sólo por el tiempo requerido para alcanzar los fines para los cuales los mismos han sido recogidos.

9. Que se garantice a todo individuo el derecho de acceso a los datos que le son propios.

Se recomienda la creación de una entidad para que, en el ámbito administrativo, vele por la observancia de los principios antes mencionados.

Debe señalarse que quedan expresamente excluidas de la legislación en referencia, las informaciones o datos meramente estadísticos, o sea aquellos que por su naturaleza genérica, no permiten relacionar a una persona específica con los mismos, o la lesión de bienes o intereses jurídicos protegidos de alguna persona, ni confieran a nadie un derecho subjetivo sobre tales informaciones o datos.

Por otra parte, esta legislación no tendría efectos sobre los bancos de datos controlados o gestionados por entidades públicas que sean regidos por leyes especiales.

Esta legislación puede ser aprovechada para definir el valor probatorio de las pruebas informáticas, ya sean discos, cintas, archivos o soportes magnéticos e inclusive los documentos que imprimen los computadores, así como los procedimientos judiciales relacionados con la materia.

Finalmente deben especificarse las actividades que serán tipificadas como delitos informáticos y por exclusión, aquellas de las cuales sólo derivará responsabilidad civil. En este último caso, deberían definirse supuestos de responsabilidad objetiva, para lo cual -en nuestro concepto- debe considerarse la informática como una actividad que crea riesgos para los titulares de los datos electrónicamente tratados, razón por la cual, quien ha creado el riesgo, o sea el controlador o gestor de bancos datos debe asumir la responsabilidad civil dimanante del daño ocasionado por el sistema, salvo que compruebe que el mismo es el

resultado del actuar del propio perjudicado, de un tercero por quien no debe responder o por caso fortuito o fuerza mayor ajena a la cosa.

BIBLIOGRAFÍA

1. Alterini, A.A. 1987. Contornos actuales de la Responsabilidad Civil. Abeledo Perrot, Buenos Aires.
2. Barrera, A.C. 1996. Nociones de Operaciones Bancarias, Panamá.
3. Bergel, S.D. Informática y Responsabilidad Civil, 1989. Informática y Responsabilidad Civil, Colección Informática y Derecho, Aportes de doctrina Internacional. Volumen 2, Ediciones Depalma, Buenos Aires.
4. Bollini Shaw, C. y Boneo Villegas, E.J. 1990. Manual para Operaciones Bancarias y Financieras. Tercera Edición, Abeledo Perrot, Buenos Aires.
5. Bonfanti, M.A. 1980. La costumbre como fuente del Derecho Bancario y en particular el papel que desempeña la costumbre internacional al respecto. En: FELABAN 1980. Cuaderno de la Biblioteca FELABAN No. 8, Editorial Kelly, Bogotá.
6. Borda, A. Responsabilidad por daños provenientes de la informática. En: Responsabilidad por daños, Homenaje a Jorge Bustamante Alsina 1990. Tomos I y II. Abeledo Perrot, Buenos Aires.
7. Borja Soriano, M. 1991. Teoría General de las Obligaciones, Editorial Porrúa, S.A., México. D.F.
8. Brown, R. 1985. Banca electrónica. Tomo I. FELABAN.
9. BusinessWeek. 1995. El dinero del futuro. En: Revista Summa Internacional , No. 60. EDIMEDIOS-SYCOM, S.A., Cali.
10. Bustamante Alsina, J. 1993. Teoría general de la Responsabilidad Civil. 8a. Abeledo Perrot, Buenos Aires.
11. Bustamante Alsina, J. 1992.Responsabilidad Civil y otros estudios. doctrina y Comentarios de Jurisprudencia. Tomo II, Abeledo Perrot, Buenos Aires.
12. Cano Martínez de Velasco, J.I. 1986. La renuncia a los derechos. Bosch, Casa Editorial, S.A., Barcelona.
13. Carreño N. M. 1990. Auditoría, seguridad y fraude en informática. En: FELABAN, No. 4, Editorial Kelly, Bogotá.
14. Castro Lechtaler, A. 1989. Los nuevos servicios de telecomunicaciones, su implicación en el ámbito bancario. En: FELABAN 1989. Revista FELABAN, No. 72. Editorial Kelly, Bogotá.
15. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL). 1986. Carácter definitivo de las transferencias electrónicas de fondos. En: FELABAN 1986. Revista FELABAN No. 60. Editorial Kelly, Bogotá.
16. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL). 1986. Problemas Jurídicos que plantean

las transferencias electrónicas de fondos. En: FELABAN 1986. Revista FELABAN No. 60. Editorial Kelly, Bogotá.

17.Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL). 1986. Valor jurídico de los registros computarizados. En: FELABAN 1986. Revista FELABAN No. 60. Editorial Kelly, Bogotá.

18.Correa, C. M. 1989. El derecho informático en América Latina, Colección Informática y Derecho, Aportes de doctrina Internacional. Volumen 2, Ediciones Depalma, Buenos Aires.

19.Correa, C.M., Bato, H.N., Czar de Zaldueno, S. y Nazar Espeche, F.A. 1987. Derecho informático. Ediciones Depalma, Buenos Aires.

20.Del Moral, O. 1993. Apuntes de clase. Curso de Responsabilidad Civil dentro de la Maestría en Derecho con Especialización en Derecho Privado de la Universidad de Panamá.

21.Del Moral, O. 1994. La Responsabilidad Civil de los bancos y sus empleados ante el manejo negligente de sus cuentas bancarias. Ponencia presentada durante el Seminario sobre Actualización del Derecho Bancario Panameño organizado por el Movimiento de Abogados Profesión y Ley el día 13 de abril de 1994.

22.Del Moral, O. 1996. Naturaleza e implicaciones legales del almacenamiento tecnológico de documentos. Ponencia presentada durante el Seminario sobre derecho informático organizado por el Movimiento Nueva Generación Jurídica en febrero de 1996.

23.Delpiazzo, C. 1990 .Legislación sobre Informática con referencia a la actividad bancaria en América Latina. En: Memorias Felabán, No. 4, Diciembre de 1990.Editorial Kelly, Bogotá.

24.Denninger, E. 1987. El derecho a la autodeterminación informativa. Problemas actuales de la documentación y la informática jurídica. Edición dirigida por Antonio Pérez Luño, Actas del Coloquio Internacional celebrado en la Universidad de Sevilla, el 5 y 6 de marzo de 1986. Editorial Tecnos, Madrid.

25.Díaz Ramírez, E. 1983. Contratos bancarios. Editorial Temis, Santa Fe de Bogotá.

26.Eckstein, P. 1989. Seguridad y control del centro de procesamiento electrónica de datos. En: FELABAN 1989. Revista FELABAN No. 73. Editorial Kelly. Bogotá.

27.Espino González, M.A. 1995. Temas actuales del derecho. 1a edición, Volumen I. Editorial Presencia, Santa Fe de Bogotá.

28.Estevil, L.P. 1989. La Responsabilidad Contractual. Tomo 2, Volumen 1, Parte Especial, Bosch Casa Editorial, Barcelona.

29.Franco, R. 1990. SWIFT (Sociedad para la telecomunicación interbancaria mundial). En: Asociación Bancaria de Panamá 1990. Revista Centro Financiero, No. 38.

30.Frosini, V. 1988. Informática y Derecho. Editorial Temis, Bogotá.

31.Garrigues, J. 1982. Curso de Derecho Mercantil. Tomo I, Madrid.

32.Ghersi, C.A. 1995. Modernos conceptos de Responsabilidad Civil. Biblioteca Jurídica Dike, Medellín.

33.Giannantonio, E. 1989. El valor jurídico del documento electrónico, Colección Informática y Derecho, Aportes de doctrina Internacional. Volumen 2, Ediciones Depalma, Buenos Aires.

34.Giannantonio, E. 1989. Transferencias electrónicas de fondos y autonomía privada, Colección Informática y Derecho, Aportes de doctrina Internacional. Volumen 2, Ediciones Depalma, Buenos Aires.

35.Glen de Tobón, M. Londoño Hoyos F. Y Rodríguez, A. 1983. Influencia de la informática en la interpretación del orden jurídico. En: FELABAN 1983. Revista FELABAN No. 48. Editorial Kelly, Bogotá.

36.González, N. 1992. SWIFT (Society of Worldwide Interbank Financial Telecomunication). En: Asociación Bancaria de Panamá 1992. Revista Centro Financiero No. 53.

37.Guerrero Mateus, M.F. y Santos Mora, J.E. 1993. Fraude informático en la Banca, Aspectos criminológicos. Editorial Jesinea, Santa Fe de Bogotá.

38. Herrera, T. 1985. Apuntes de clase del Curso de Derecho Bancario dentro de la Licenciatura en Derecho y Ciencias Políticas de la Universidad Santa María la Antigua.

39.Izquierdo Tolsada, M. 1989. La Responsabilidad Civil del profesional liberal. Editorial Reus, S.A.

40.Jaén, E. 1996. Avances recientes de la informática aplicadas a las actividades bancarias en Panamá. En: Asociación Bancaria de Panamá 1996. Revista Centro Financiero No. 73.

41.Jijena Leiva, R.J. 1992. Chile, La protección penal de la intimidad y el delito informático. Editorial Jurídica de Chile.

42.Lombardi T., J.E. 1965. La Responsabilidad Extracontractual Civil en el Derecho Panameño. Universidad de Panamá, Facultad de Derecho y Ciencias Políticas, Panamá.

43.Lopes da Silva, L.E. 1980. El secreto bancario frente a las centrales de crédito y a las centrales de riesgo. En: FELABAN 1980. Cuaderno de la Biblioteca FELABAN No. 8. Editorial Kelly, Bogotá.

44.Malagarriga, J.C. 1970. El secreto bancario. Abeledo Perrot, Buenos Aires.

45.Mazeud, H., Mazeud, L. y Tunc A. 1977. Tratado teórico y práctico de la Responsabilidad Civil, Delictual y Contractual. Tomos I, Vol. 1 y 2 y III, Vol. 2 Ediciones Jurídicas Europa América, Buenos Aires.

46.Meján, L.M.C. 1984. El secreto bancario. Biblioteca FELABAN, Editorial Excélsior, Bogotá.

47.Meján, L.M.C. 1994. El Derecho a la intimidad y a la informática. 1a edición. Editorial Porrúa, S.A., México, D.F.

48.Memorias FELABAN, No. 4. Diciembre de 1990. Editorial Kelly, Bogotá.

49.Messina de Estrella Gutiérrez, G.N. 1989. La Responsabilidad Civil en la era tecnológica. Abeledo Perrot, Buenos Aires.

50.Monroy Cabra, M.G. 1995. Tratado de Derecho Internacional Privado. Editorial Temis, Bogotá.

51.Parellada, C. A. 1990. Daños en la actividad judicial e informática desde la Responsabilidad Profesional. Editorial Astrea, Buenos Aires.

52.Peña Castrillón, G. 1979. Algunos aspectos jurídicos de la automatización bancaria. En: FELABAN 1979. Cuadernos de la Biblioteca FELABAN No. 2, Editorial Kelly, Bogotá.

53.Quiroga Lavié, H. Los Derechos Humanos y su Defensa ante la Justicia. Editorial Temis, Santa Fe de Bogotá.

54.Responsabilidad por daños. 1990. Homenaje a Jorge Bustamante Alsina. Tomos I y II. Abeledo Perrot, Buenos Aires.

55.Rivera S., R. 1987. Plan de contingencia en informática: el caso de Nacional Financiera. En: Asociación Mexicana de Bancos. Congreso Latinoamericano de Automatización Bancaria 1987. Revista FELABAN No. 63, Bogotá.

56.Rodríguez Azuero, S. 1990. Contratos bancarios: Su significación en América Latina. Biblioteca FELABAN. 4ta edición. Bogotá.

57.Román, Alejandro. 1993. Apuntes de clase, Curso de Instituciones de Crédito dentro de la Maestría en Derecho con Especialización en Derecho Privado de la Universidad de Panamá.

58.San Miguel, L. G. 1992. Estudios sobre el Derecho a la intimidad. Editorial Tecnos, S. A. Madrid.

59. Serrano Rodríguez, J. 1989. Análisis de decisiones de inversión en tecnología bancaria. En: Felaban 1989. Revista Felaban No. 72. Editorial Kelly, Bogotá. 180 págs.

60.Superintendencia Bancaria de Colombia. 1990. Riesgos de los sistemas de computación y telecomunicaciones de los bancos. En: Asociación Bancaria de Panamá 1990. Revista Centro Financiero No. 40.

61.Tamayo Jaramillo, J. 1986. De la Responsabilidad Civil (de los perjuicios y su indemnización). Tomo II, Editorial Temis, Bogotá.

62.Tamayo Jaramillo, J. 1986. De la Responsabilidad Civil. Las presunciones de las Responsabilidad y sus medios de defensa. Tomos I y II. 2a edición. Editorial Temis, Bogotá .

63.Trigo Represas, F.A. 1987. Responsabilidad Civil de los profesionales. Editorial Astrea, Buenos Aires.

64.Van Hewck, P. 1989. TRASEC: Sistema nacional de la seguridad para la transferencia electrónica de fondos en Bélgica. En: FELABAN 1989. Revista FELABAN No. 72. Editorial Kelly, Bogotá D.E.

65.Villamizar, F. 1996. La red INTERNET y sus efectos en la banca de hoy. En: Asociación Bancaria de Panamá 1996. Revista Centro Financiero, No. 74.

66.Villegas, G.C. 1989. Compendio jurídico, técnico y práctico de la actividad bancaria. Tomo I Editorial De Palma, Buenos Aires.

67.Zagaris, Bruce. 1994. Como combatir y prevenir fraudes y tretas en transacciones bancarias internacionales. Ponencia presentada durante el Congreso Latinoamericano de Comercio Exterior, Asociación Bancaria de Panamá, Panamá, julio 25 a 28 de 1994.

68.Zannoni, E.A. 1993. El Daño en la Responsabilidad Civil. 2a edición. Editorial Astrea, Buenos Aires.